THE AUTHENTICATION OF ELECTRONIC EVIDENCE

Allison Rebecca STANFIELD

LLB (Hons) (QUT), LLM (QUT)

Submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Faculty of Law

Queensland University of Technology

January 2016

Keywords

Evidence Act, evidence, electronic evidence, digital evidence, business records, Hearsay Rule, metadata, hard drive, computer, backup tape, the Cloud, social media, privilege.

Abstract

The various Evidence Acts throughout Australian jurisdictions contain a number of provisions facilitating proof of electronic evidence. In its 2005 Report on Uniform Evidence Law, the Australian Law Reform Commission considered whether the uniform Evidence Acts should be amended to impose a more rigorous requirement for the presumption of reliability and accuracy of computer-produced evidence. The Commission reported that given the division of opinion on this issue and the lack of empirical evidence justifying a more rigorous test for the reception of evidence in electronic form, the Commission was persuaded that a case for change has not been made out. In the ten years since that Report there have been many advances in technology and more opportunities for the courts to test the reliability of electronic evidence in comparison with the reliability of paper based evidence. This proposal challenges the findings of the Commission and in doing so will investigate the nature and origins of electronic evidence, how it has been treated by courts since its inception and whether existing legislation sufficiently protects the integrity of electronic evidence in contemporary times.

Table of Contents

List of Figures

List of Abbreviations

Abbreviation	Description
BD	Blu-ray Disc
BD-ROM	Blu-ray Disc Read Only Memory
BD-RW	Blu-ray Disc Re-Writable
CAD	Computer-aided Design
CD-ROM	Compact Disc Read Only Memory
CD-RW	Compact Disc-ReWritable
CF	Compact Flash
DBMS	DataBase Management Systems
DVR	Digital Video Recorder
DVD-ROM	Digital Versatile Disc Read Only Memory
DVD-R	Digital Versatile Disc Readable
DVD-RW	Digital Versatile Disc Re-Writable
ESI	Electronically Stored Information
GIF	Graphics Interchange Format
HD	High Definition video
IM	Instant Messenger
JDBC	Java Database Connectivity
JPEG	Joint Photographic Experts Group
MP3	MP3 is an audio-specific format that was designed by the Moving Picture Experts Group (MPEG)
ODBC	Open Database Connectivity
PDF	Portable Document Format
PVR	Personal Video Recorder
RSS	Really Simply Syndication

Abbreviation	Description
SD	Standard Definition video
SIM	Subscriber Identity Card
SQL	Structured Query Language
SMS	Short Message Service, which is a text messaging service component of phone, Web, or mobile communication systems.
TIFF	Tagged Image File Format
USB	Universal Serial Bus

Table of Cases

Cases

List of Statutes

Statutes

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

QUT Verified Signature

Signature:

Date: 28 January 2016

Acknowledgements

Computer technology has always fascinated me, and as a lawyer, I developed a passion for the ways in which technology has confounded and challenged the lawyers who are confronted with this relatively new paradigm. The law changes slowly, and this is clearly the case when it comes to developing new laws to cope with the changes in technology. In fact, it is difficult, if not impossible, to keep up.

This paper has been researched and compiled over a number of years and I would like to firstly thank my supervisors, Professor Bill Duncan and Professor Sharon Christensen whose sage counsel since the genesis of my thesis, has been invaluable. I would also like to thank my paralegals who have helped proof various versions, and check numerous citations. In particular, I would like to thank Nhi Y-Pham whose genius will not go unnoticed in the 'real world'. Additionally, I thank Kat Flynn, Sam Harris, Simon Moses and Laurence Henly for their assistance.

While researching and writing this paper, I also had my 'day job' running e.law and I would like to thank my colleagues and staff who stepped up and brilliantly fulfilled their roles while I was writing.

I thank my family, in particular my husband Steven Gates and my daughters Sara, Georgia and Amelia for always being there for me.

1. CHAPTER 1 – INTRODUCTION

1.1 Overview

[1.1.1.1] The present rules surrounding documentary evidence have been developed over centuries, and these rules were developed to apply to hard copy documents.[1] Electronic evidence is fundamentally different to hard copy, such that the rules of evidence surrounding documentary evidence need to be re-examined. Indeed, a computer disc is different from a filing cabinet in which hard copy documents are stored because the information is actually embedded in the storage medium.[2]

[1.1.1.2] Following a lengthy review of evidence law by the Australian Law Reform Commission ('ALRC'), the Commonwealth enacted the *Evidence Act 1995* (Cth),[3] which has subsequently been enacted in, New South Wales,[4] Victoria,[5] Tasmania,[6] the Australian Capital Territory[7] and the Northern Territory[8] (the *Uniform Evidence Acts*). The other states have their own Evidence Acts.[9]

[1.1.1.3] The admissibility of electronic evidence has largely rested upon whether a computer was functioning correctly or not, and the rebuttable presumptions contained in the *Uniform Evidence Acts* ss 146 and 147 do allow for such presumptions to be rebutted should it be shown that the computer was malfunctioning at the time the evidence was created. However, these presumptions do not look at the security around the computer system to determine if it is robust enough to confirm that the evidence taken from the system is what it purports to be. The foundations upon which these presumptions have been built, fail to take into account that it is much easier to change electronic evidence without detection, than it ever was in the hard copy world. Further, the author of the document may not even be aware that changes have been made. The Hearsay Rule, which was developed by the courts to ensure that out of court statements did not make their way into evidence as truth of the assertions made in

[1] Hard copy documents can included media such as paper, parchment and vellum, although in modern times paper has become the most popular form of medium. For the sake of brevity, throughout this thesis, paper will be referred to as the default form of hard copy documents.
[2] *Innovative Health Group Inc. v Calgary Health Region* 2008 ABCA 219 (CanLII) (Madam Justice Conrad).
[3] Which commenced on 18 April 1995.
[4] *Evidence Act 1995* (NSW), which commenced on 1 September 1995.
[5] *Evidence Act 2008* (Vic), which commenced on 1 January 2010.
[6] *Evidence Act 2001* (Tas), which commenced on 17 December 2001.
[7] *Evidence Act 2011* (ACT), which commenced on 1 March 2012.
[8] *Evidence (National Uniform Legislation) Act* (NT), which commenced on 1 January 2013.
[9] *Evidence Act 1929* (SA), *Evidence Act 1977* (Qld) and *Evidence Act 1906* (WA).

those statements, has not been subject to more stringent testing as a result of this new form of evidence. Indeed, it is perhaps easier to admit hearsay than it ever has been.

[1.1.1.4] The ALRC *Report on Uniform Evidence Law*, delivered on 5 December 2005,[10] did consider whether the Evidence Acts adequately addressed the reliability and accuracy of computer-produced evidence. Later, in DP69,[11] the ALRC asked 'whether the uniform Evidence Acts should be amended to impose a more rigorous requirement for the presumption of reliability and accuracy of computer-produced evidence?'.[12]

[1.1.1.5] In 1998, the Queensland Law Reform Commission recognised that electronic evidence, such as email, does require a different method of authentication compared to hard copy authentication.[13]

[1.1.1.6] The issue was highlighted because the *Evidence Act 1929* (SA) s 45C appeared to have a more comprehensive provision compared to the *Evidence Act 1995* (Cth) s 146 'in ensuring that a device producing a document is in itself not prone to error'. This issue is explored further in section 2.13.

1.2 The History of Documentary Evidence

[1.2.1.1] The history of documentary evidence is long and convoluted. The law surrounding documentary evidence has been developed over centuries and has evolved around paper documents. By contrast, electronic evidence has only been in standard use for around 20 years, however, these centuries-old laws are still being applied to electronic evidence.

[1.2.1.2] Chapter 2 examines the history of documentary evidence to set the background to then determine whether these rules can still be applied today to electronic evidence. In particular, the rule that the content of documents is hearsay, and is not admissible unless it falls within one of the exceptions to the Hearsay Rule, including the Business Records Exception.

[1.2.1.3] The use of documents appeared as a means to record transfers of land. During the Norman's feudal system, a charter replaced the ceremony of presenting a twig to the grantee

[10] Australian Law Reform Commission, *Uniform Evidence Law*, Report No 102 (2005).
[11] Australian Law Reform Commission, *Review of the Uniform Evidence Act*, DP 69 (July 2005).
[12] Ibid at 16.
[13] Queensland Law Reform Commission, *The Receipt of Evidence by Queensland Courts: Electronic Records*, Issues Paper WP No 52 (August 1998), p89.

of land. However, general distrust of writing meant witnesses were called, regardless of any inconsistencies.

[1.2.1.4] Documents bearing the King's seal became indisputable and this led to common seals being used, which then became a method of authentication.

[1.2.1.5] Early cases involving deeds saw the witnesses to the deed on the jury, as early as 1208 to 1489. This led to 'Trial by Charters' where there could be no claim without a charter, and attesting witnesses had to be called to prove its authenticity. The court could not go beyond the Charter and this gave rise to the origin of estoppel by deed and the parol evidence rule. Oral evidence had no place in trial by charter.

[1.2.1.6] The doctrine of estoppel by deed developed where solemn and unambiguous statements in deeds were taken as binding.

[1.2.1.7] The parol evidence rule emerged to prevent oral evidence being admitted to vary a deed. The rationale was that verbal variations to the document could not be admitted to alter the agreement which had been committed to writing and sealed by the parties. Exceptions to the parol evidence rule arose to permit showing that a contract was void and to expose fraud. Soon after, the *Statute of Frauds*[14] was enacted in England during the 17th Century, which allowed documents to be authenticated if signed by the parties, rather than affixing a seal. Certain contracts were covered, including contracts for the transfer of interest in land, and even today, this requirement still exists, albeit in a more modern form.

[1.2.1.8] Prior to the introduction of machines which could reproduce documents exactly, the best evidence rule applied, which meant that the party wishing to rely upon the document had to produce it or account for its absence.

[1.2.1.9] As to documents which were not sealed or signed, their contents constituted hearsay, so unless documents are being tendered as real evidence, they had to be tendered through a witness who could attest as to their contents. A document could not, on its face, prove itself. Several exceptions to the Hearsay Rule for documentary evidence developed over time, most notably the Business Records Exception. This Rule provides that as long as the document was produced in the ordinary course of business, the person who authored the

[14] *An Act for the Prevention of Frauds and Perjuries 1677* (Eng) ('Statute of Frauds').

document did not need to attest that the document is what it purports to be, but rather a person who has personal knowledge of the facts can testify about the records.

[1.2.1.10] Legislative provisions have codified and even modified these common law rules that developed over time.

[1.2.1.11] Finally, proving that a signature on a document is or is not a forgery is an important aspect of authentication, such that there is now a body of forensics that just specialises in handwriting. Although there are a wide range of electronic signatures that may be applied to an electronic document, there does not yet appear to be an electronic equivalent of the handwritten signature. However, the National Electronic Conveyancing System will substantially change the way conveyancing is conducted[15] and seemingly, will be the first time electronic signatures will be used for the transfer of an interest in land. This leads to first question, which is whether electronic signatures are adequate for electronic documents?

1.3 About Electronic Evidence

[1.3.1.1] Electronic evidence is very different to paper based evidence, and these differences are explained in Chapter 3. Essentially, electronic evidence is comprised of three main elements, the first being binary data, the second being a storage device on which to store that binary data and thirdly, software to read and interpret the binary data.

[1.3.1.2] Although electronic evidence has only been used, in a standard commercial sense, for around 20 years, the forms of electronic evidence are constantly changing. Social media and cloud computing technologies were not common 20 years ago, and are gaining such widespread acceptance that they will be standard in 20 years' time, and may even be superseded by other forms of technology. Chapter 3 explains these various types of changing technologies, which are critical to understand before considering the application of the rules of evidence to them.

[1.3.1.3] One aspect of electronic documents, which do not exist in paper documents is metadata. Metadata is electronic information about other electronic data and is created by and embedded in electronic documents. 'Meta-data can be used to ascertain the author and origin

[15] Sharon Christensen, 'A National Law for Electronic Conveyancing - New Rules and Practices for Queensland' on *Thompson Reuters Online Insider* (24 May 2013) <http://blog.thomsonreuters.com.au/2013/05/a-national-law-for-electronic-conveyancing-new-rules-and-practices-for-queensland/> at 20 November 2014.

of a document, the existence of any attachments, and whether the document was sent or received by any particular individual. The information which is contained in the meta-data is not visible on a print-out of the relevant document, which shows only the face content and does not disclose the layers of electronic data beneath the visually readable information'.[16] Metadata would include information such as the date of creation of the document, the date sent, received and so on.

[1.3.1.4] The volume of electronic evidence is increasing exponentially each year[17] and the fact that storage media is becoming less and less expensive, and more easily accessible, means that the traditional method of adhering to a document destruction and retention policy, may prove too costly and complex for most commercial corporate entities. It is far easier and takes up less time for staff, if all data is simply kept for an indefinite period. This, in itself, causes problems, largely due to storage media constantly being upgraded or large tracts of data being stored on inappropriate media. Further, if an entity becomes involved in litigation and has to undertake discovery, this is when the real issues with data storage become evident. 'Where' is the data stored, 'how' can it be retrieved, 'whose' data is relevant, 'what' data is needed and 'when' are the relevant date periods. The volume of data to be reviewed is significantly greater today than it was when hard copy was used. Not only are users creating more documents (email and text messaging is much more casual, users are content to discuss issues via these methods rather than commit to the traditional letter writing or even telephone calls), but the ways in which documents can be created are ever changing. While email has become the default 'letter' in the business world, the children of today see email as old fashioned and communicate with one another via social media and text messaging. All of this material, whether formal or not, may comprise later evidence to be adduced.

[1.3.1.5] The benefit of having documents in electronic format, however, is that the greater volume can be more easily searched. The new technologies that are being created to identify and find documents based on concepts, or having the technology be 'trained' to recognise relevant documents, is shaping the way for how documents will be located and reviewed in litigation in the future. These new technologies and their application to the rules

[16] Per Tamberlin J in *Jarra Creek Central Packing Shed Pty Ltd v Amcor Limited* [2006] FCA [11].
[17] See further Jason R. Baron, *Law in the Age of Exabytes: Some Further Thoughts on 'Information Inflation' and Current Issues in E-Discovery Search*, 17 Rich J.L & tech. 9 (2011).

of evidence, are examined further in Chapter 5.

[1.3.1.6] 'Clever' technology is emerging that allows duplicate documents, including 'near duplicates' that are similar but not identical, such as versions of a contract, or the scanned hard copy of a printed document compared with the Microsoft Word version, to be identified so lawyers are only reviewing a document once, or can see all versions of a document together. Likewise, technology allows emails in the same 'thread' or 'chain' to be grouped together so a reviewer can see these all at once.

[1.3.1.7] Electronic evidence is persistent and can appear in any number of locations. All of these various copies are identical to each other, so if one set of data is not available, it may be possible to obtain the evidence from another location.

[1.3.1.8] The most striking element of electronic evidence is that is dynamic and changeable and this is what gives most concern when it comes to authentication.

[1.3.1.9] Given the fast pace of change in technology, electronic evidence may be stored on a medium which can become redundant, or the software upon which it was created, is no longer supported. This can lead to problems with accessibility and potential corruption of the evidence if it is not properly migrated to more modern systems.

[1.3.1.10] Electronic evidence today is being dispersed in ever increasing different locations and jurisdictions from the residence of document owners. Only a short time ago, a business stored its electronic evidence on servers and other computers in its offices. Today, many businesses are outsourcing their data storage to 'the Cloud'. The Cloud is a term used to describe vendors who 'rent' computer hardware and/or software to entities; this is an alternative to entities buying their own computer hardware and software. The Cloud Provider (vendor) can create several 'virtual' computers on one computer hard drive, thereby maximising the amount of space on that computer. These virtual computers are what are rented out to customers. The Cloud business is growing, as organisations see the benefit of renting computer space rather than buying computer hardware and software and also having to have infrastructure, communications, security and of course human resources to maintain the hardware and software. The Cloud leads to legal issues that have not been considered previously, such as jurisdictional issues, potential confidentiality issues, data ownership and loss of data if a Cloud Provider becomes insolvent.

[1.3.1.11] For evidence to be available, it needs to be accessible, and with electronic evidence, it is possible that evidence may simply be inaccessible. If it is inaccessible, it may either be too expensive to retrieve, or it may simply be impossible to retrieve because it has been corrupted. This is explained further in section 3.3.8.

[1.3.1.12] There are various types of storage media, most of which today are capable of storing huge quantities of data. For example, a one terabyte external hard drive can be purchased for less than one hundred dollars. One terabyte of data would constitute about 700,000 three inch floppy disc drives, which were commonly used in the 1990's. It is difficult to gauge how many documents would comprise one terabyte of data, given data sizes vary so greatly, however, if one document comprised 1 megabyte, then around one million documents would comprise one terabyte.

[1.3.1.13] Content is created in various formats, the most common being in word processing formats, Portable Document Format ('PDF'), email and on social media.

[1.3.1.14] Finally, databases are a form of content that is stored as separate items and arguably a 'document' is only created when a script is run within software to produce a report from the database. The form of databases varies considerably.

[1.3.1.15] Chapter 3 examines the various types of storage media, content and the differences between hard copy and electronic information. This leads to the next question, which is whether the current rules of evidence adequately recognise the unique nature of electronic evidence.

1.4 Analysis of Existing Rules of Evidence

[1.4.1.1] When forms of electronic evidence first came before the courts in Australia, the question often determined by the court was whether a particular form of evidence was a 'document' as defined by the *Uniform Evidence Acts*. Various types of electronic material was, therefore, considered by the courts and much was, indeed, determined to be 'documents' for the purpose of admission as evidence. These cases are considered in Chapter 4.

[1.4.1.2] Chapter 4 also considers documentary evidence as being subject to the Hearsay Rule, largely because the contents of document comprise human generated information and unless the person who created that content can give evidence that the document is what it

purports to be, then the evidence will not be admissible. There are certain exceptions to the Hearsay Rule, one being the Business Records Exception. This exception essentially provides that as long as the record was generated in the ordinary course of business, someone with knowledge of the records, generally a senior member of the business can give evidence which leads to the admission of the documents into evidence. This rule developed as a common sense approach where employees leave businesses, only to have records tendered after their departure. In a matter involving documents over a lengthy period of time, it makes practical sense to have a person with knowledge of the business tender all documents, rather than through several different people, many of whom may no longer work for the business.

[1.4.1.3] The common law has defined a document very broadly and when considering electronic 'documents', broader still. Indeed, what would have been considered a filing cabinet full of documents in the paper world has been held to be a 'document' for the purposes of the *Uniform Evidence Acts*. The case law on the meaning of ‘document’ is considerable and complex. Chapter 4 considers a few salient cases to attempt to rationalise the courts' views upon that definition, for the purposes of this thesis.

[1.4.1.4] The Business Records Exception determines the way in which business records are admitted into evidence. The way in which the courts have determined what is a 'record', and what constitutes business records, are also considered in Chapter 4. The question raised is whether the definition of ‘document’ in the *Uniform Evidence Acts* sufficient to cover electronic evidence and, in particular, does it sufficiently identify the natures of electronic evidence in that it comprises both content and storage media?

1.5 Discovery/Disclosure of Electronic Evidence

[1.5.1.1] There are two components to evidence being admissible in court. First, is whether the evidence is, indeed, admissible? Whether the evidence is admissible depends initially on whether it is relevant to a fact in issue in the proceeding. Secondly, for a document to be admissible, it must be authentic, that is, it must be what it purports to be.[18]

[1.5.1.2] If electronic evidence is to be properly authenticated, it must be collected in such a way that it does not compromise the integrity of the evidence. This is particularly

[18] *National Australia Bank Ltd v Rusu* (1999) 47 NSWLR 309, 312 (Bryson J).

important where evidence is seized. A specialist science known as 'computer forensics' has developed which focuses on the collection of electronic evidence in a 'forensically sound' manner. This process is examined in Chapter 5. A computer forensics expert, through computer analysis, can show that evidence was not changed from the time it was obtained, either by consent or by some form of court order such as a search warrant or an Anton Piller order. Computer forensics can also be used to show that metadata has changed, thereby making it likely that the evidence itself was changed. However, with the take up of cloud computing where data is now stored on 'virtual' servers where information is much more dynamic, 'computer forensics' plays less of a role compared to the way in which the Cloud Provider stores information, and the contract it has with the end user. For example, a user's contract with a Cloud Provider may provide that the user's data is not their own, that the Cloud Provider, 'owns' it, that the data may be stored offshore, in a different jurisdiction. Certainly, data that is stored on a 'virtual' computer is not accessible in the same way as data that is stored on a physical hard drive. This is explored further in Section 3.5.8.

[1.5.1.3] Data storage and retrieval then leads to consideration of electronic discovery (some jurisdictions use the term 'discovery' while others use 'disclosure'). In Australia, electronic discovery has been practised since the 1990s, and in 1999, the practice was first regulated by the Supreme Courts of New South Wales and Victoria by the implementation of practice notes about the use of technology in litigation.[19] The method then was mostly by scanning paper documents and data coding metadata about each document, so that databases could be used to search and find relevant documents. Now that almost all evidence is created electronically and exchanged electronically, not only does it makes sense to obtain the electronic evidence for review during discovery, but also the electronic version is the best evidence and contains more information than a paper copy generated by a print out. Australian courts have issued Practice Notes/Directions dealing with electronic discovery. These are reviewed in Chapter 5.

[1.5.1.4] When exchanging electronic documents, lawyers are concerned that privileged documents are not inadvertently discovered and if they are, privilege is not waived. The way

[19] In 1999, the Supreme Court of Victoria issued Practice Note No. 3 of 1999 and the Supreme Court of New South Wales issued Practice Note No. 105. These have been replaced by the following current practice notes: Australia, Supreme Court of New South Wales, *SC Gen 7 Supreme Court – Use of Technology*, 9 July 2008, Australia, Supreme Court of New South Wales, Practice Note SC Eq 11, 22 March 2012 and Australia, Supreme Court of Victoria, *Practice Note, No 1 of 2007 Guidelines for the Use of Technology in any Civil Matter*.

in which courts have dealt with the issue of privilege is considered in Chapter 5.

[1.5.1.5] Many lawyers neither understand technology, nor the way in which electronic documents are processed. Chapter 5 provides an overview of how this is done, and focuses on the way in which technology is continually improving to ensure that vast volumes of electronic documents can be reviewed cost effectively, and only those that are relevant to the issues in the case, are highlighted for review. Lawyers can find the evidence that is relevant to the matter, quickly and easily, and by ensuring that the original, ('native'), evidence is used, rather than a paper copy.

[1.5.1.6] Education is the key to providing lawyers with the necessary skills to review electronic documents in a way that is inexpensive and efficient for their client. Many courts and judges have criticised how discovery now comprises a large component of litigation costs. Indeed in some jurisdictions, such as in the Equity Division of the Supreme Court of New South Wales, the court has issued a practice direction[20] stating that 'the Court will not make an order for disclosure of documents until the parties to the proceedings have served their evidence on the other party to the litigation, unless there are exceptional circumstances necessitating disclosure'.[21]

[1.5.1.7] Discovery can be a critical step in the litigation process, however, does the discovery process provide sufficient safeguards to ensure that the integrity of evidence remains intact?

[1.5.1.8] Chapter 5 also looks at how parties may claim legal professional privilege over documents, which do not then need to be discovered. This leads to the next question, which is whether, for documents to which legal professional privilege applies, are there sufficient protection measures in place for retrieval of evidence on electronic media that contains privileged information?

1.6 Authentication of Electronic Evidence

[1.6.1.1] If the document is relevant and authentic, the evidence may nevertheless be inadmissible if it is excluded by a rule that provides for the exclusion of particular kinds of

[20] Australia, Supreme Court of New South Wales, *Practice Note SC Eq 11*, 22 March 2012.
[21] Ibid s 4.

evidence such as the Hearsay Rule.[22]

[1.6.1.2] The reality is that electronic evidence for transactions or documents may only ever exist in electronic format. Documentary evidence is by itself, hearsay, and requires a witness to tender the document and testify as to its contents. Conversely, real evidence is evidence that 'speaks of itself', rather than evidence of what someone said.[23] Therefore, many electronic documents will comprise an element of each. Once evidence has been found to be admissible, the next question the court will consider is the weight that will be given to the evidence. It has been suggested that generally, the court uses two criteria to measure the evidentiary weight of electronic records. The first is probative value: is the electronic record relevant and has authorship, authenticity, correct operation and reliability been established? The second criterion is whether, according to the rules of evidence, the electronic record been collected and handled correctly.[24]

[1.6.1.3] With respect to probative value, records must be relevant to the matter at hand and all relevant electronic records must be presented. To meet those requirements, it must be demonstrated that the procedures used to collect electronic records were reasonable and robust enough to discover obvious, lost or hidden material.

[1.6.1.4] Electronic evidence is different to paper, and by its very nature gives rise to complex questions about its integrity, reliability and accuracy. The very question of authentication comes down to whether electronic evidence is the same as it was when it was created. The very nature of electronic evidence means that it can be altered by a third party with access to it. However, this does not mean that the content or context has changed.

[1.6.1.5] Authenticating electronic evidence is mainly left to the court to determine if the document is what it purports to be, and if it is admitted, what weight the court will give the evidence. There is scant case law in Australia about the authentication of electronic evidence.

---

[22] Ibid.

[23] *R v Penney* (2002) 163 CCC (3d) 329 at [35] and [41].

[24] Yatan Dahiya and Sunita Sangwan, 'Developing and Enhancing the Security of Digital Evidence Bag' (2014) 1(2) *International Journal of Research Studies in Computer Science and Engineering (IJRSCSW)* 14-25. See also George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008) at 36 where he commented that '.. to learn about the authenticity of digital information we must ask questions about the attributes of the information object in question. First, is it associated with the identity it purports to be associated with? Next, there are questions about the constancy of the information in a record. Constancy or immutability of information, called "integrity", is a key attribute of authenticity of information.'

Thus, the law in the United States of America, England and Wales and Canada has been examined in Chapter 5, to determine whether their existing rules of evidence have been applied consistently and adequately across the board. Commentators have suggested that the authentication of electronic evidence is merely a 'trivial showing' and that it is the system in which the evidence is created and stored, upon which the courts should concentrate when looking to authenticate electronic evidence.[25]

[1.6.1.6] A vast problem facing commercial organisations is how to archive electronic information in such a way that it can be later admissible in court if required. The Electronic Discovery Reference Model[26] ('EDRM') has recently added Information Governance as the first component of the electronic discovery life cycle. This is as a result of companies being involved in litigation and finding that in order to first obtain the pool of information that is potentially relevant to a discovery, they first need to find the information itself. A legacy of the burgeoning amount of cheap electronic storage space has meant that old archival regimes have not been kept, with the result that electronic information can reside in a number of disparate locations. This can mean a costly exercise in retrieval of the information. The EDRM is examined further in Chapter 5.

[1.6.1.7] Although the *Uniform Evidence Acts* have abolished the best evidence rule, which allowed 'copies' of documents to be admitted, the practicality of electronic information is that a 'copy' is not a straightforward concept. A good example of this is information stored as records in a database. A piece of information stored as a field in a database is meaningless unless it is put into context with other pieces of information from the database. In order for the other fields of information to be pulled together, software is required in order to query the various database fields and present them as a report or other record. A good example of this would be accounting software. The various pieces of financial information are stored as fields within the database and then at the end of each month after various manual entries have been completed, the software can produce reports such as profit and loss statements. To simply store each field of information in isolation from the software can render the information meaningless. This is a common problem facing many organisations today; as software becomes obsolete,

[25] George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008) 48.

[26] The *Electronic Discovery Reference Model*, refer Electronic Discovery Reference Model website: <http://www.edrm.net> as at 11 September 2015, was launched in May 2005 to address the lack of standards and guidelines in the e-discovery market.

record managers are faced with the problem of having to preserve information in a way that preserves the original data and that the meaning of the information is not changed by the preservation process.

[1.6.1.8] Archive bodies such as the National Archives and the various State government archive bodies, along with libraries, have issued guidelines on the preservation of electronic records. There are also standards in place, such as HB171-2003 Guidelines for the Management of IT Evidence, which outline standards for the preservation of evidence and the obligation to provide records which includes:

> (a) Understand regulatory, administrative and best-practice obligations to produce, retain and provide records;
> (b) Understand the steps that can be taken to maximise the evidentiary weighting of records and the implications of not doing so; and
> (c) Understand regulatory constraints to the retention and provision of records.

[1.6.1.9] The archiving procedures for electronic records are very different to archiving procedures for hard copy records. Even digitising hard copy records is a relatively straightforward process compared with archiving existing electronic records. Standards for record keeping are set out in AS ISO 15489.1. Further, AS/NZS ISO/IEC 17799:2001 Information technology sets out a code of practice for information security management. It provides that information classification requires organisations to develop an information classification scheme that indicates the need, priorities and degree of protection and label electronic records accordingly. An organisation's information classification and labelling scheme must include an assessment of the potential evidentiary significance of electronic records.

[1.6.1.10] The biggest challenge facing archival of electronic records is the emulation of the software long after it has been de-commissioned. Organisations often need to de-commission software for a number of reasons. For instance, commonly software licence fees may be prohibitively expensive to keep in place if an enterprise decision has been made to move to other software for its business functions. The software vendor may have gone out of business or may no longer provide support and maintenance for the software. In these circumstances, the organisation must archive its data in such a way that the software generated reports can be replicated. This is difficult to do without the original software in place. There are still no standards in place which allow for information to be extracted from databases and

placed into a non-proprietary format for long term archival. Even if such standards were in place, the fact the information was created from a proprietary format in the first place, means that the proprietary software would need to be the subject of examination to prove that the software produced the reports correctly.

[1.6.1.11] This leads to the next question, which is: are the current rules of authentication for documentary evidence, sufficient to apply to electronic evidence?

1.7 Summary & Conclusion

[1.7.1.1] The analysis of this area of the rules of evidence pose the following questions to be answered. These are highlighted as the analysis raises each question, and these are answered in the final Chapter 7.

Question 1:
Are the laws recognising electronic signatures adequate for evidentiary purposes for documents?

Question 2:
Is the definition of 'document' in the Uniform Evidence Acts adequate for the purposes of electronic evidence and, in particular, does it appropriately identify the nature of electronic evidence in that it comprises both content and storage media?

Question 3:
Should the Business Records Exception, in its present for in the *Uniform Evidence Acts*, continue to apply to electronic evidence, or does it need modification?

Question 4:
Does the discovery process provide sufficient safeguards to ensure that the integrity of evidence remains intact?

Question 5:
For documents to which legal professional privilege applies, are there sufficient protection measures in place for retrieval of evidence on electronic media that contains privileged information?

Question 6:
Do the presumptions in *Uniform Evidence Acts* ss 146 and 147 need modification to reflect the way in which electronic evidence is generated?

Question 7:
Are the current rules of authentication for documentary evidence, adequate to apply to electronic evidence?

2. CHAPTER 2 – THE HISTORY OF DOCUMENTARY EVIDENCE

2.1 Introduction

[2.1.1.1] A study of the history of documentary evidence reveals that it is convoluted and inconsistent. However, two rules around documentary evidence arose to circumvent forgery. The first is that the original evidence be used whenever possible and, the second, that the document be authenticated by adducing evidence that the document is what it purports to be. These basic rules have subsequently been diluted.

[2.1.1.2] Documentary evidence can be used in evidence to prove the truth of its contents, or it can be real evidence. Real evidence is not hearsay, as it is evidence of itself. For example, maps generated by Google Earth were recently found by the United States of America Court of Appeals for the 9th Circuit, to be real evidence, and not hearsay.[27]

[2.1.1.3] Further, as stated by Stone and Wells,[28] contemporaneous documentary evidence can be used as a medium of proof.

[2.1.1.4] A document does not necessarily need to have paper as a medium of proof. In *R v Daye,*[29] the court stated that 'it is impracticable to base any distinction upon the material bearing the inscription'. Indeed, it is the symbols upon the medium which comprise the evidence, and 'to change a symbol changes the thought which it transmits and the ease with which symbols may be changed or misrepresented calls for great precautions to ensure that they have not been so changed or misrepresented.'[30] This is particularly the case when considering electronic evidence.

[2.1.1.5] The rules surrounding documents have produced three main categories (a) authenticity: if the contents of a document are in question, then the original must be produced, (b) admissibility: what evidentiary rules apply to the document, that is, is it being tendered for the truth of its contents and if so, is it hearsay, and (c) is it a deed?: if the document is a deed, then certain presumptions have developed regarding sealing of a deed.

[27] *U.S. v. Lizarraga-Tirado* (2015 WL 3772772 (9th Cir. June 18, 2015).
[28] Julius Stone and William Wells, *Evidence Its History and Policies* (Butterworths, Australia: 1991) 303.
[29] [1908] 2 KB 333, 340.
[30] Stone and Wells, above n 28, 468.

2.2 Genesis of Documents as Evidence

[2.2.1.1] The use of documents as evidence grew over time and initially oral practices were dominant due to Germanic influences which held writing in distrust.[31] The 5th to 11th Centuries saw formal legal acts of the 'sala', which was a declaration of an intention to transfer land; and 'gewerida', a ritualistic handing over of possession of land, that was usually performed in public.[32] Under the Normans' feudal system, a ceremony was held whereby the grantor of a transfer of land would cut some turf and break a twig off a tree, and give these to the grantee as a symbolic gesture. The twig and turf were eventually replaced by the charter that recorded the transfer.[33] However, given the distrust of writing during this time, it continued to be the case that witnesses were called regardless of any inconsistencies with what had been written down.[34]

[2.2.1.2] The next era in the use of documents as evidence saw the seal become more commonly used. Documents with the King's seal were seen as indisputable, and this spread to documents with common seals, which in turn, led to the growing authority of charters, and seals becoming the method of authenticity.[35] In many *quo warranto* cases, claims without charters were held inadmissible.[36]

[2.2.1.3] In medieval times, early methods of contract enforcement included wager of law where the defendant would deny the debt supported by the oaths of eleven other people and this would suffice to defeat the plaintiff's claim.[37] An exception to wager of law was where there was a sealed charter, referred to as a rule 'as old as compurgation itself'.[38] In the 12th Century, a creditor could prove their claim by battle or by charter.[39] Trial by ordeal or battle

---

[31] On use of documents before the 14th Century, see Andreas Heusler, *Institutionen des deutschen Privatrechts* (Duncker & Humblot, Germany, 1885), quoted in John H Wigmore, 'A Brief History of the Parol Evidence Rule' (1904) 4 *Columbia Law Review* 338, 339.

[32] Heather MacNeil, 'From the memory of the act itself. The evolution of written records as proof of jural acts in England, 11th to 17th Century' (2006) 6 *Journal of Archival Science* 313, 314.

[33] Ibid 315.

[34] Ibid 314.

[35] Ibid 317.

[36] Michael T Clanchy, *From memory to written record: England, 1066-1307* (Cambridge Press, United Kingdom: 2nd ed, 1990) 35-37, quoted in MacNeil, above n 32, 316.

[37] William M McGovern, 'Contract in Medieval England: The Necessity for Quid pro Quo and a Sum Certain' (1969) 13(3) *The American Journal of Legal History* 173, 201.

[38] William M McGovern, 'Contract in Medieval England: Wager of Law and the Effect of Death' (1968) 54 *Iowa Law Review* 19, 29.

[39] Ranulf de Glanville, *Tractatus of Glanvill* (United Kingdom: 1188), Translated as *Treatise on the Laws and Customs of England*, cited in McGovern, above n 37, 201.

was also sometimes used, although more rational forms of trial were gaining favour by this time. Trial by jury was not used for issues of debt because members of the jury were expected to use only their personal knowledge. Jury trials were therefore left for matters of common knowledge.[40]

[2.2.1.4] In the early 13th Century, judges determined factual questions.[41] A plaintiff in debt had to have a charter or a suitable witness to prove their claim. Early cases regarding deeds saw the witnesses to the deed on the jury, as early as 1208 until as late as 1489.[42] A witness to a deed, according to the popular conception, was not necessarily one who had seen it executed, but one who was willing to give it credit by his name.[43]

[2.2.1.5] In *Evidence It's History and Policies,*[44] Stone and Wells refer to 'Trial by Charters' where there could be no claim without a charter, and attesting witnesses had to be called to prove its authenticity. The court would not go beyond the charter. The charter would be conclusive, and this is the origin of estoppel by deed and the parol evidence rule. The original rule was not that parol evidence could not be introduced to vary a charter, only that oral evidence had no place in trial by charter.

2.3 Estoppel by Deed

[2.3.1.1] Use of the seal gave rise to 'estoppel by deed', where solemn and unambiguous statements in deeds were taken as binding.[45]

[2.3.1.2] However, the written deed remained inferior to oral ceremonies.[46] For example,

---

[40] McGovern above n 38, 20.
[41] James B Thayer, 'The Jury and its Development. II' (1892) 5 *Harvard Law Review* 295, 298.
[42] Ibid 302.
[43] Ibid.
[44] Stone and Wells, above n 28, 24-25.
[45] See *Bowman v Taylor* [1834] 2 Ad & El 278 concerning an indenture in which it was recited that the plaintiff had invented some improvements in the construction of looms and had His Majesty's patent and that the plaintiff had agreed to permit the defendants to use the invention for a price. The defendants did not perform their part so the plaintiff went to the court. The defence from the defendants was that invention was not a new invention alleging that the plaintiffs therefore had no right to give the licence. It was held there was estoppel by matter of recital so the defendants could not deny that the plaintiff had invented these improvements. Earlier cases referred to included *Hayne v Maltby* (1789) 3 TR 438, which the judges distinguished because there, the articles of agreement did not recite the invention was original, only that the plaintiffs were assignees of the patent, therefore, no estoppel in that case; *Oldham v Langmead* (1796) 3 TR 439, Lord Kenyon would not allow the patentee to show the invention was not a new one against his own deed; *Lainson v Tremere* (1834) 110 Eng Rep 1410 shows there may be estoppels by recital in a deed. Exception of fraud or illegality*: Greer v Kettle* [1938] AC 156.
[46] MacNeil, above n 32, 315.

in the case of *Rye v Humby*[47] it was said that 'the charter is naught but a little ink and parchment which will not avail to override my will at the time of livery'. There remained a distinction between the effect of a deed in creating estoppel and its effect in supplying evidence that could be rebutted. If it was to create an estoppel, it had to be brought forward before the jury was called as it would be a bar to the action, whereas if used as evidence it had to be advanced to the jury. As trial by jury increased, the use of sealed documents as well as other documents, became more common.

[2.3.1.3] By the end of the Middle Ages 'the custom was adopted of stamping a written agreement of the parties with a seal so as to make its authenticity indisputable'.[48] In *Sharington v Strotton*,[49] it was held that a sealed document is of a higher nature than other evidence. In *Lord Cheyney's Case*,[50] the court said 'for it would be full of great inconvenience that none should know by the written words of a will what construction to make or advice to give, but it should be controlled by collateral averments out of the will'.

[2.3.1.4] By the 1600s, the 'modern rule of indisputability is established for all transactions affecting realty'.[51] Courts started to accept the written word as being more reliable.[52]

[2.3.1.5] Stone and Wells suggest[53] that documents as the basis for a claim were viewed as important to regulate in terms of admission. In contrast, oral testimony was to be revealed by 'the judgment of God' and oral evidence only came to be regulated when it was established the jury could only give a verdict on the evidence of witnesses sworn on oath, in the case not based on other knowledge they might have. This explains why rules as to the admission of documents in evidence are ancient and sometimes anomalous.

[2.3.1.6] Today, a deed is a recognised form of agreement evidencing a transaction for

[47] (1314) 8 Y B Edw 11.
[48] Alberto Luis Zuppi, 'The Parol Evidence Rule: A Comparative Study of the Common Law, the Civil Law Tradition, and Lex Mercatoria' (2007) 35 *The Georgia Journal of International and Comparative Law* 233, 236.
[49] (1565) 75 Eng Rep 454.
[50] (1591) 6 Co Rep 68; 77 Eng Rep 158 (Court of Wards and Liveries).
[51] John H Wigmore, 'A Brief History of the Parol Evidence Rule' (1904) 4 *Columbia Law Review* 338.
[52] For the history of the printing press and the shift in paradigm that this wrought, see David J Harvey, *The Law Emprynted and Englysshed, The Printing Press as an Agent of Change in Law and Legal Culture 1475-1642*, (Hart Publishing, Oxford, 2015); See also Ian Williams, "He Creditted More the Printed Booke – Common Lawyers Receptivity to Print 1550 to 1640" (2010) 28 *Law and History Review* 38.
[53] Stone and Wells, above n 28, 25.

value or a gift, and may or may not have consideration to bind the bargain. A deed can be unilateral (deed poll) or signed by more than one party (indenture), as is required for the transfer of an interest in land, and deeds could be varied in writing only.[54] The requirements of the 'seal', or signature, both in handwriting and electronically (as recognised by the *Electronic Transactions Acts*, see section 2.14.5 below), are critical when examining authenticity and admissibility.

2.4 The Parol Evidence Rule

[2.4.1.1] The parol evidence rule prevents a party to a written contract from presenting extrinsic evidence that amends or contradicts the written terms. The rationale for the rule is that because the parties have reduced their agreement to writing, extrinsic evidence of past agreements or terms should not be considered when interpreting that written agreement.

[2.4.1.2] The Parol Evidence Rule, which still exists today, appeared in the early 1600s, just before the enactment of the *Statute of Frauds*.[55] In a quote from *Isabel Countess of Rutland's Case*[56] in 1606:

> It would be inconvenient that matters in writing made by advice and on consideration, and which finally import the certain truth of the agreement of the parties should be controlled by averment of the parties to be proved by the uncertain testimony of slippery memory.[57]

[2.4.1.3] In *Earl of Suffolk v Greenvill*,[58] the court warned against the reliance on oral testimony finding 'it very dangerous to admit the contents and sufficiencies of deeds to be proved by the testimony of witnesses, the construction of the deeds being the office of the Court; and the fact touching execution pertained only to the proof of witnesses'. Langbein[59] commented that this could mean that the original deed was to be produced to prove the transaction, but it more likely meant that oral evidence of a deed was unacceptable and a true copy, at least, of the deed would need to be produced.[60]

[54] *Berry v Berry* [1929] 2 KB 316.
[55] *An Act for the Prevention of Frauds and Perjuries 1677* (Eng).
[56] (1572) 6 Co Rep 52; 77 Eng Rep 332.
[57] Ibid per Popham CJ.
[58] (1641) 3 Ch Rep 89; 21 Eng Rep 738 [92].
[59] John H. Langbein, 'Historical Foundations of the Law of Evidence: A View from the Ryder Sources' (1996) 96 *Columbia Law Review* 1168.
[60] Ibid 1181.

[2.4.1.4] The parol evidence rule extended to non-sealed contracts,[61] as evident in *Meres et al v Ansell et al,*[62] where the Court of Common Pleas said that 'no parol evidence is admissible to disannul and substantially to vary a written agreement'.[63]

[2.4.1.5] Thayer suggests the case applied a rule from *Jones v Morley*[64] in which an oral declaration could not be used to challenge in a fine levied pursuant to a covenant. Cole reports that Popham CJ found 'for every contract or agreement ought to be dissolved by matter of as high a nature as the first deed'.[65]

[2.4.1.6] According to the decision in *Shore v Wilson,*[66] the rule was about promoting legal certainty.[67] In *Jacobs v Batavia & Gen. Plantations Trust Ltd,*[68] it was held that 'parol evidence will not be admitted to prove that some particular term, which had been verbally agreed upon, had been omitted (by design or otherwise) from a written instrument constituting a valid and operative contract between the parties'.

[2.4.1.7] Similarly, in *Bank of Australasia v Palmer,*[69] Lord Morris explained the rule as '[p]arol testimony cannot be received to contradict, vary, add to or subtract from the terms of the written contract, or the terms in which the parties have deliberately agreed to record any part of their contract'.[70] The House of Lords has since admitted extrinsic evidence on the 'matrix of facts' of the background of the agreement known to the parties at the time.[71]

[2.4.1.8] In Australia, the courts have followed the House of Lords. The High Court considered the admissibility of extrinsic evidence in *Codelfa Constructions Pty Ltd v State Rail*

---

[61] James B Thayer, *A Preliminary Treatise on Evidence at the Common Law* (Boston Little Brown, United States of America: 1898), ch10.
[62] (1771) 3 Wils 276, cited in Thayer, above n 61, 402.
[63] Thayer, above n 61, 403.
[64] (1696) 2 Salk 677, quoted in James B Thayer, 'The Jury and its Development. III' (1892) 5 *Harvard Law Review* 295, 387.
[65] Wigmore, above n 51, quoted in Tony Cole 'The Parol Evidence Rule: A Comparative Analysis and Proposal' (2003) 26 *University of New South Wales* Law *Journal* 680.
[66] (1842) 8 Eng Rep 450.
[67] Ibid, cited in Alberto Luis Zuppi, 'The Parol Evidence Rule: A Comparative Study of the Common Law, the Civil Law Tradition, and Lex Mercatoria' (2007) 35 *The Georgia Journal of International and Comparative Law 233* 233, 237.
[68] [1924] 1 Ch 287.
[69] [1897] AC 540.
[70] Ibid 545; see also *Rabin v Gerson Berger Association* [1986] 1 All ER 374.
[71] See *Prenn v Simmonds* [1971] 3 All E.R. 237, 1383-84 (Lord Wilberforce); Note the English Law Commission, *Parol Evidence Rule*, Working Paper No. 154, (1986) questioned whether the rule had been in fact largely destroyed.

Authority of NSW.[72] Mason J (as he then was) confirmed the rule to be that extrinsic evidence is only admissible if the language is ambiguous or susceptible to more than one meaning.

2.5 Exceptions to the Parol Evidence Rule

[2.5.1.1] Exceptions to the parol evidence rule include (a) to prove the contract is void, one can plead outside the contract or (b) fraud.[73]

[2.5.1.2] The exception, to prove the contract was void and that one can plead outside the contract, was manifested by *Collins v Blantern*[74] where it was held, for the first time, that illegality of consideration not appearing on the face of a bond was a good defence. Wilmot CJ said:

> The law will legitimate the showing it void ab initio and this can only be done by pleading;… what strange absurdity would it be for the law to say that this contract is wicked and void, and in the same breath for the law to say you shall not be permitted to plead the facts which clearly show it to be wicked and void.[75]

[2.5.1.3] This was approved by Lord Mansfield in *Pole v Harborn*.[76]

[2.5.1.4] Fraud as a defence was upheld in 1601-1602 in *Fermor's Case* in the Court of Chancery.[77] In this case, the Lord Keeper and two Chief Justices decided that 'they thought it necessary that all the justices of England and Barons of the Exchequer should be assembled for the resolution of this great case'. The prevalent issue was whether the plaintiff was barred from having relief in Chancery by a fine. It was agreed unanimously that the fine was not a bar: 'it was answered that it would be a greater mischief… if fines levied on such covin and practice should bind'.[78]

[2.5.1.5] Thayer noted[79] that by the end of the 17th Century, Courts of Equity had found ways to use extrinsic intention and even direct oral expressions. Part of this was that the Court of Equity did not use juries who would be biased by such evidence. For example, in *Strode v*

[72] (1982) 149 CLR 337. This case was followed by the High Court in *Royal Botanic Gardens & Domain Trust v South Sydney City Council* (2002) 186 ALR 189, 293.
[73] Ibid, ch10.
[74] (1767) 2 Wils 347, cited in Thayer, above n 61, 406.
[75] Ibid (Wilmot CJ), cited in Thayer, above n 61, 406.
[76] (1782) 9 East 415, cited in Thayer, above n 61, 406.
[77] (1601-2) 3 Co 77, cited in Thayer, above n 61, 407.
[78] Ibid 408.
[79] Thayer, above n 61, 389.

Russell[80] the court observed: 'This is not like the case of evidence to a jury who are easily biased by it, which this court is not'.

[2.5.1.6] By the end of the 18th Century, it was clear that the courts required a contemporaneous written record of many transactions to counter the possibility of fraud. The primary purpose of a written record to support oral testimony as a vehicle of proof was further acknowledged in cases that did not concern the *Statute of Frauds*.[81]

2.6 The Statute of Frauds

[2.6.1.1] The admissibility of a written document into court proceedings became relevant upon the enactment of the *Statute of Frauds*[82] in the 17th Century. This was a watershed moment for documents as evidence. Notably, the transaction was constituted by the documents, not just proven, and the documents, to be admissible, did not require a seal.

[2.6.1.2] Traditionally, the *Statute of Frauds* required a signed writing in the following circumstances:

> (a) Contracts in consideration of marriage;
> (b) Contracts that cannot be performed within one year;
> (c) Contracts for the transfer of an interest in land. This includes transfers of land, but also contracts where an interest in land is disposed such as a mortgage or an easement;
> (d) Contracts by the executor of a will to pay a debt of the estate with his own money;
> (e) Contracts for the sale of goods over a certain value; and
> (f) Contracts in which one party becomes a surety (acts as guarantor) for another party's debt or other obligation.[83]

[2.6.1.3] Some of the original *Statute of Frauds* provisions still exist today, in a more modern form. Written records generally, became a more robust way to prove facts, due to the increasing number of transactions between strangers, not just with family and friends.

[2.6.1.4] The case that is said to have led to the enactment of the *Statute of Frauds* was *Slade's Case*[84] Here, there was a shift from trial by wager to trial by jury which shifted the advantage to the plaintiff in proving parol promises in debt cases.

[80] (1708) 3 Rep Ch 169; 21 Eng Rep 758.
[81] *An Act for the Prevention of Frauds and Perjuries 1677* (Eng) 29 Car 2.
[82] Ibid.
[83] Ibid, s IV.
[84] (1602) 4 Co Rep 92; 76 Eng Rep 1074.

[2.6.1.5] Teeven[85] identified the *Statute of Frauds* as a method of remedy of a defendant's disadvantage by attempting to 'make those arrangements apparent to third parties by requiring that certain agreements be memorialised in written form'.

[2.6.1.6] The preamble to the *Statute of Frauds* provides that the Act is 'for prevention of many fraudulent practices which are commonly endeavored to be upheld by Perjury and Subornation of Perjury'.[86] Chapter 4 of the *Statute of Frauds* listed the agreements which needed to be evidenced in writing and be signed by the person to be charged or their agent and included:

> (a) Any promise by an executor or administrator to answer damages out of their own estate;
> (b) Any promise to answer for the debt, default, or miscarriage of another person;
> (c) Any agreement made in consideration of marriage;
> (d) Any contract or sale of lands, tenements, or hereditaments, or any interest in or concerning them; and
> (e) Any agreement not to be performed within a year from its making. [87]

[2.6.1.7] The leading case following the *Statute of Frauds* is said to be *Birkmyr v Darnell*,[88] in which it was said:

> If two come to a shop and one buys, and the other, to gain him credit, promises the seller, if he does not pay you, I will; this is a collateral undertaking and void without writing, by the Statute of Frauds.[89]

[2.6.1.8] It was held in *Crosby v Wadsworth*[90] that contracts concerning land, must be in writing. *Tisdale v Harris*,[91] applying the *Statute of Frauds*, became authority that contracts concerning the sale of goods, wares or merchandise required writing.

[2.6.1.9] Later, in *Goss v Nugent,*[92] Denman CJ noted that the purpose of the *Statute of Frauds* was to exclude all oral evidence as to contracts for the sale of lands, so that any contract sought to be enforced must be proven by a written contract only. In this case, Denman CJ also

[85] K. M. Teeven, 'Seventeenth Century Evidentiary Concerns and the Statute of Frauds' (1983) 9 *Adelaide Law Review* 252, 253.
[86] *Statute of Frauds* (1677) 29 Car 2 c1.
[87] Ibid 4.
[88] (1704) 1 Salked 27.
[89] Ibid 27, 28.
[90] (1805) 6 East 602; 102 Eng Rep 1419.
[91] (1838), 20 Pick. (Mass.) 9.
[92] (1833) 2 LJ KB 127; 110 Eng Rep 713, 716.

explored the interpretation of the parol evidence rule and formulated the rule as follows:

> If there be a contract which has been reduced to writing, verbal evidence is not allowed to be given of what passed between the parties, either before the written instrument was made or during the time that is was in a state of preparation, so as to add to or subtract from, or in any manner to vary or qualify the written contract.[93]

[2.6.1.10] In *Queen's Caroline case*,[94] Abbott CJ found that:

> It is a rule of evidence as old as any part of the common law of England that the contents of a written instrument, if it be in existence, are to be proved by the instrument itself and not by parol evidence.[95]

[2.6.1.11] The increasing relevance of documents as evidence in litigation was apparent in the case of *Roberts v Clifton*[96] in which the trial judge overruled the objection of the plaintiff's counsel to admit the document that showed the defendant had asked for work from the plaintiff on his employer's request. This case demonstrates the perceived reliability of documentary evidence over oral testimony. This premise was borne out in decisions over subsequent years.

[2.6.1.12] Secondary evidence can often play a prevalent role in proving the authenticity of documents. Cases such as *Maxwell v Sharp*[97] and *Clerk v Dolling*[98] illustrate that witnesses were called upon to testify to signatures and the author's handwriting in order to testify as to the authenticity of documents.

[2.6.1.13] Similarly, Lord Tenterden CJ in *Vincent v Cole*[99] warned against reliance on witness testimony noting that:

> What is in writing shall be proved only by the writing itself: my experience has taught me the extreme danger of relying on the recollection of witnesses, however honest, as to the contents of written instruments: they may be so easily mistaken, that I think the purposes of justice require the strict enforcement of the rule.[100]

[2.6.1.14] The premise that a document must be produced if its contents are to be referred

---

[93] Ibid.
[94] *Queen's Caroline case* (1819) 1 State Tr NS 949 (Abbott CJ), quoted in Stone and Wells, above n 28, 24.
[95] However, there are exceptions to this rule such as those regarding a lease, see *Farmer d. Earl v Rogers* (1755) 95 Eng Rep 666.
[96] (1755) 15 Ryder NB 19, as quoted in Langbein, above n 59, 1183.
[97] (1755) Sayer 187, 96 Eng Rep 847.
[98] (1755) 15, Ryder 29, 30.
[99] (1828) M & M 257; 173 Eng Rep 1151.
[100] Ibid [258] (Lord Tenterden CJ).

to in oral testimony was illustrated by *MacDonnell v Evans.*[101] In the cross-examination of a witness for the plaintiff, counsel for the defendants asked a question concerning a letter. These questions were objected to by counsel for the plaintiff and the court disallowed the question on the basis that it assumed there was a document in existence that should have been proved by production of the original document itself. Thus developed the parol evidence rule.

2.7 Superiority of Written Evidence

[2.7.1.1] In *The Superiority of Written Evidence,*[102] Salmond considers how traditionally there was a well-marked tendency in the law to set up an external measure of evidence and test of proof. A key element of this tendency was to make the relation between evidence and proof a matter of law, with the division of evidence into three classes, namely; record, writing, and averment. Evidence of record and writing were said to be a higher class than that of averment.

[2.7.1.2] Salmond gives two leading applications of this rule.[103] The first; that where matter in writing and matter in averment are opposed to each other, the former must prevail. The second; that where evidence in writing is available, evidence of averment is inadmissible. The premise that a deed cannot be annulled or altered except by deed is clearly guided by the principle of superiority in writing. Salmond, in *Essays Jurisprudence and Legal History,*[104] notes a plaintiff saying: 'We have put forward a deed which is admitted in court and you have nothing in hand to certify the court of the truth of your statement, but only make an assertion; judgment as of undefended'.[105]

[2.7.1.3] Superiority of written evidence over its verbal counterpart is also evident in the doctrine of estoppel by deed. For example, in a further case cited by Salmond, it was held that 'nothing contained in a writing can by any exception of the parties be removed.[106] Further, Salmond notes that these principles have not been extended from deeds to other writings.[107]

[2.7.1.4] The rule that 'matter in writing must prevail over matter of averment' is found in the doctrine of the inadmissibility of parol evidence to qualify the effect of written

[101] (1852) 11 CB 930; 138 Eng Rep 742.
[102] John W Salmond, 'The Superiority of Written Evidence' (1890) 6 *Law Quarterly Review* 75
[103] Ibid 262.
[104] John W Salmond, *Essays in Jurisprudence and Legal History* (Littleton Colorado F B Rothman, United States of America, 1987).
[105] Ibid 46.
[106] 22 Edward I 436, quoted in Salmond, above n 102, 50.
[107] Salmond, above n 102, 2.

instruments.[108] This has been extended to all forms of writing, not just a deed. Salmond makes reference to this,[109] where an attempt to exclude evidence that a deed absolute on its face, meant to be conditional on marriage, was unsuccessful.

[2.7.1.5] Sir Geoffrey Gilbert, in *Law of Evidence,* [110] emphasised that documents were ranked from high to low in terms of credibility, from Acts of Parliament, records of common-law courts, public records with a seal, public records without a seal, and then public matters not of record, private writings such as deeds and finally wills. It is noted that deeds ranked higher than other written documents as they are presumed to have been made on good consideration.[111]

[2.7.1.6] The legal effect of an alteration to a deed can only be accomplished at law by a deed of variation, but in equity, a deed could be varied in writing.[112]

2.8 Best Evidence Rule

[2.8.1.1] The common law best evidence rule has now been abolished by the *Uniform Evidence Acts.*[113] However, the old common law rule stated that 'the party who claims to put the contents of a writing in evidence must produce it, or account for its absence'.[114]

[2.8.1.2] The best evidence rule has its origins *Omychund v Barker,*[115] where Lord Harwicke stated that no evidence was admissible unless it was 'the best that the nature of the case will allow'. Secondary evidence, or the production of proof other than by the original, have produced exceptions to this rule. The rule is traceable to the ancient method of trial by charter where there could be no trial without the charter.[116] The rule transformed into a rule

[108] Ibid 7.
[109] Salmond, above n 102, 4.
[110] Geoffrey Gilbert, *The Law of Evidence* (Catherine Lintot Publishing, United Kingdom, 1791) 7.
[111] Ibid 17.
[112] See *Berry v Berry* [1929] 2 KB 316, 319 (Swift J) '...courts of equity have always held themselves at liberty, to allow the rescission or variation by a simple contract of a contract under seal by preventing the party who has agreed to the rescission or variation from suing under the deed'.
[113] *Evidence Act 1995* (Cth), s 51; *Evidence Act 1995* (NSW), s 51; *Evidence Act 2008* (Vic), s 51; *Evidence Act 2001* (Tas), s 51; *Evidence Act 2011* (ACT), s 51; *Evidence (National Uniform Legislation) Act* (NT), s 51; *Evidence Act 1929* (SA) s45C contains modifications to the best evidence rule, *Evidence Act 1977* (Qld) does contain exceptions to the best evidence rule, including s 95 Admissibility of statements produced by computers; *Evidence Act 1906* (WA) s 73A contains an exception to the best evidence rule for reproductions;
[114] *R v Frankland* (1863) Le & Ca 276; 169 Eng Rep 1394 (Erle J).
[115] (1745) 1 Atk, 21, 49; 26 ER 15, 33.
[116] Ibid 470.

that applied to both formal and informal documents.

[2.8.1.3] In *Dr Leyfield's Case*,[117] it was suggested that originals were required, 'he ought to shew the original deed to the Court', and that it ought to be proved by witnesses 'that it was sealed and delivered'.[118]

[2.8.1.4] The rule was based on the doctrine of profert (one of pleading rather than evidence): 'At common law, if a claim or defence were based on an instrument under seal ('deed'), the party relying upon it was required to make profert i.e. indicate his willingness to bring it into court.'[119] The opposing party would then have the document read to him and it would become part of the pleadings. 'If the document were lost or other satisfactory reason given for its non-production, profert was excused'.[120] However, profert did not apply in criminal cases, and in civil cases it was limited to:

> (a) Sealed instruments, letters of administration, testamentary letters; and
> (b) Documents on which a claim or defence was founded (therefore, most of documentary evidence used today would be outside the scope of profert).[121]

[2.8.1.5] The rule is said to have been 'christened' by Chief Justice Holt in *Ford v Hopkins*,[122] where he said:

> The best proof that the nature of this thing will afford is only required. The basic, though largely unarticulated, premise which may be said to underlie most contemporary justifications of the rule is the tremendous importance of the written word to the law.[123]

[2.8.1.6] Preference for writing is clearly illustrated by the *Statute of Frauds* and the parol evidence rule. Therefore, it became important to have the most accurate evidence of writing possible. The rule only applied if the content of the document was in question.

[2.8.1.7] In *Steyner v The Burgesses of Droitwich*,[124] Holt CJ said 'This is but a copy [of the original deed]; and though an old manuscript found among the evidences of a family, may

[117] (1572) 10 Co Rep 88; 77 Eng Rep 1057.
[118] Ibid 9.
[119] John W Strong and Edward W Cleary, 'The Best Evidence Rule: An Evaluation in Context' (1965) 51 *Iowa Law Review* 825, 831.
[120] Ibid.
[121] Ibid.
[122] (1795) 1 Salk 283; 91 Eng. Rep. 249 (KB).
[123] Ibid.
[124] (1688-1710, 1738) Holt KB 290; 90 Eng. Rep. 1059.

be evidence, because it is an original, yet a copy would not, for it is liable to the mistake of the transcriber.'[125]

[2.8.1.8] There are contrasting views as to whether oral testimony or documentary proof constitutes the best evidence. Gilbert's *The Law of Evidence* treated the best evidence rule 'as a unifying theme'.[126] This was attacked by Jeremy Bentham in *The Rationale of Judicial Evidence*[127] who claimed that '[w]itnesses are the eyes and ears of justice'.[128] In *What is the Law of Evidence?*[129] Twining concluded that in the 20th Century rules of evidence should be seen only as 'a mixed group of exceptions to a principle of freedom of proof',[130] and that there was no principle that written evidence should be given more weight than witness testimony.

[2.8.1.9] In The Jury and the Exclusionary Rules of Evidence,[131] Morgan wrote:

> The requirement that a documentary original must be produced as evidence of its content has its root in the ancient substantive law, which identified the legal consequences of a document with the document itself. The method of trial where the authenticity of the writing was in dispute, was by deed witnesses before the court, and not by jury. As trial by jury gradually displaced trial by documents the requirement of profert in pleading made mandatory the production of the original in court.

2.9 Development of the Hearsay Rule

[2.9.1.1] In *The History of the Hearsay Rule*,[132] Wigmore noted[133] that the rule that required an extra witness to testify began in the 1500s, but only became fully developed by the early 1700s. However, it had already been the case since early modes of trial that those who were on the witness stand could speak only of what was within their personal knowledge. In the 1600s, hearsay statements were often received, even against opposition as was the case in the *Duke of Norfolk's Trial*[134] in 1571, where there was no exclusion of hearsay statements and

[125] Ibid 623 (Holt CJ).
[126] Gilbert, above n 110, cited in Eilis S Magner 'The Best Evidence – Oral Testimony or Documentary Proof?' (1995) 18(1) *The University of New South Wales Law Journal* 67, 68.
[127] Jeremy Bentham, *A Treatise on Judicial Evidence Extracted from the Manuscripts of Jeremy Bentham*, Esq (Baldwin, United Kingdom: 1st ed, 1825).
[128] Ibid 226.
[129] William Twining, *Rethinking Evidence* (North West University Press, Illinois: 2nd ed, 2006).
[130] Ibid 188.
[131] Edmund M. Morgan, 'The Jury and the Exclusionary Rules of Evidence' (1937) 4(2) *The University of Chicago Law Review* 247.
[132] John H Wigmore, 'The History of the Hearsay Rule' (1904) 7 *Harvard Law Review* 437, 437.
[133] Ibid 444.
[134] I How. St. Tr 958, cited in Wigmore, above n 132, 444.

various letters were used against the accused.

[2.9.1.2] The hearsay doctrine continued to develop and became more regimented in the period around 1675-1690. In *Pickering v Barkley*,[135] 'a certificate of merchants' was read in court but the court desired to have the merchants brought into court to testify. Similarly in *Ireland's Trial*[136] the defendant sought to bring a document from a College in France to testify that he was there for an alibi. Atkins J said 'such evidences as you speak of we would not allow against you; therefore we would not allow it for you',[137] so thereafter the members of the College appeared to testify. In a similar manner, in *Anderson's Trial*,[138] a letter was not admitted into evidence.

2.10 The Business Records Exception

[2.10.1.1] The present day Business Records Exception allows records of businesses to be admitted into evidence without the need to have the person who created the records attend court to give evidence.[139] There are certain pre-conditions, such as the records need to be made in the ordinary course of business, and the person admitting the records must have personal knowledge of the records.[140]

[2.10.1.2] The predecessor to the current Business Records Exception is the 'shop-book rule'. During the 17th Century, it was becoming common for businesses to keep written records of their transactions and at common law, an exception to the Hearsay Rule developed known as the 'shop-book rule'.[141] This exception evolved in two branches, one as an exception for regular entries made in the course of business where the individual who made the entries was no longer available to appear as a witness. The second exception was where the entries were made by a party to the suit, notwithstanding they were available as a witness.[142] In *Doe v Turford*,[143] it was held that if books were regularly kept by a third person who was now deceased, the books could still be admitted into evidence provided the person's death and regularity of their book-keeping were established. Although the shop-book rule was abolished

[135] Ibid.
[136] 7 How. St. Tr. 79, 105. (1678), cited in Wigmore, above n 132, 446.
[137] Ibid 105.
[138] (1680) 7 How.St.Tr.8II, 865, cited in Wigmore, above n 132, 446.
[139] See for example, *Uniform Evidence Acts* s 69.
[140] Ibid.
[141] Skogstad and Koppa, 'Admissibility of Business Entries' (1958) *Wisconsin Law Review* 24, 245.
[142] Ibid.
[143] (1832) 3 B & Ad 890; 110 Eng Rep 327.

by statute in 1609, it saw a re-emergence in the 19th Century in the United States of America.[144]

[2.10.1.3] In 1879, in England, the *Bankers' Books Evidence Act of 1879* (Eng) was enacted to allow records[145] of banks to be admissible upon an affidavit of one of the superior officers of the bank, without the need to call the clerk or clerks, who made the entry or entries.

[2.10.1.4] The critical turning point in the development of an exception to hearsay was the introduction of the *Evidence Act 1938* (Eng) which mandated that certain documents could be admissible on particular conditions as exceptions to hearsay. They included the following documents: (a) baptismal certificates admissible as evidence of legitimacy in proceedings for letters of administration;[146] (b) a letter by a testator that he had not made a will,[147] a letter in which a testator expressed his dislike for a particular relative,[148] notes made by a solicitor with respect to the preparation of a will,[149] notes by a clerk in relation to a pending probate action;[150] (c) factual accounts of road or industrial accidents to a policeman;[151] (d) hospital records tracing the history of a patient's treatment;[152] and (e) statements in public documents are evidence of the facts which they assert.[153]

[2.10.1.5] In *Myers v Director of Public Prosecutions,*[154] the defendant was charged with car theft, and the prosecution wanted to admit evidence of microfilms of record cards from the car factory which recorded the engine number, chassis number and block number of each vehicle as it was being assembled and would have likely proved that the cars were stolen. The House of Lords held that these records were not admissible because they had not been brought to court by a witness who could testify to their accuracy and who had compiled them. Although the records were made in the course of duty in a business, and contemporaneously, the persons who had made them could not be shown to be dead. Unless the records could be proven to be

[144] Skogstad and Koppa, see above n 141 at 245.
[145] *Bankers' Books Evidence Act 1879* (Eng) s 3 provides that 'entries in ledgers, day books, cash books and other account books of any bank shall be admissible'. In 1980, the courts confirmed that such records included modern technology, such as microfilm, which was widely in use at that time: *Barker v Wilson* [1980] 2 All ER 81; [1980] 1 WLR 884.
[146] *Re H deed* 1949 VLR 197.
[147] *Will of Thorne* 1947 VLR 415.
[148] *Re Thompson* [1939] 1 All Eng Rep 681.
[149] *In the Estate of Powe, Decd. Powe v Barclays Bank Ltd (Powe and Others Cited)* [1955] 3 All ER 448.
[150] *In the Estate of Hill, Decd. Braham v Haslewood and Another* [1948] 2 All ER 489.
[151] *Simpson v Lever* [1963] 1 Q.B. 517.
[152] *Reed v Columbia Fur Dressers Ltd* [1965] 1 W.L.R. 13.
[153] *Wilton & Co v Phillips* (1903) 19 TLR 390 (KB).
[154] [1965] AC 1001.

true, the records had no probative value. They were not public documents as they were not open to inspection. Lord Reid said:[155]

> The witness could only say that a record made by someone else showed that, if the record was correctly made, a car has left the works bearing three particular numbers. He could not prove that the record was correct or that the numbers which it contained were in fact the numbers on the car when it was made. This is a highly technical point, but the law regarding hearsay evidence is technical and I would say absurdly technical.

[2.10.1.6] Lord Morris said that there was 'there was every reason in the present case to suppose that the workmen or mechanics concerned would make correct entries. They could have no other purpose than to do so... The existing exception to the hearsay rule which admits evidence of declarations in the course of duty is, however, subject to the firmly established condition that the death of the declarant must be shown'.[156]

[2.10.1.7] Lord Hodson did not want to extend the exception regarding public records to private records not open to inspection. Lords Pearce and Donovan dissented.[157]

[2.10.1.8] In the *Criminal Evidence Act 1965* (Eng), the Business Records Exception continued to apply, but only if the person who had made them were dead.

[2.10.1.9] The present day Business Records Exception embodies the shop-book rule, in so far as records kept in the ordinary course of business, can be admitted into evidence, without the need to call every person who made each entry. This is invaluable where records were made by employees who have subsequently left the company. The modern-day business Records Exception is explored further in section 4.4.

2.11 Public Documents

[2.11.1.1] A public documents is today defined in the Dictionary to the *Uniform Evidence Acts* as a document that:

> (a) forms part of the records of the Crown in any of its capacities; or
> (b) forms part of the records of the government of a foreign country; or
> (c) forms part of the records of a person or body holding office or exercising a function under or because of the Constitution, an Australian law or a law of a foreign country; or
> (d) is being kept by or on behalf of the Crown, such a government or such a person or body;

[155] Ibid 1019.
[156] Ibid 1028.
[157] Ibid later applied in *R v Patel* [1981] 3 All ER 94.

> and includes the records of the proceedings of, and papers presented to:
>
> (e) an Australian Parliament, a House of an Australian Parliament, a committee of such a House or a committee of an Australian Parliament; and
>
> (f) a legislature of a foreign country, including a House or committee (however described) of such a legislature.

[2.11.1.2] In *Evidence Its History and Policies*,[158] Stone and Wells noted that 'public documents' were treated differently in terms of proof and noted a requirement of production of original documents as well.[159] An exception to the rule that the original be produced in the case of a 'public document' was explored in *Mortimer v M'Callan*[160] where Lord Abin held that statutes such as the *Banker's Books Evidence Act 1879* (Eng) extended what was public to allow a copy of the original document to be the used as evidence. Similarly, the *Evidence Act 1845* (Eng)[161] allowed for some documents to be produced as a copy if they were signed or sealed in a certain way.

[2.11.1.3] Rules about the exception to hearsay in public documents:

> (1) Statements must be made by a public officer under a public duty to inquire and record facts for a public purpose: *Trade Practices Commission v TNT Management Pty Ltd*.[162]
> (2) Must be intended to be kept indefinitely: *Heyne v Fischel*.[163]
> (3) Must be open, upon reasonable terms, to public inspection: *Batlow Packing House v Commonwealth & Dominion Line Ltd*.[164]

[2.11.1.4] In *Potts v Miller*[165] the High Court held that books of a company could be admitted as evidence 'of the financial progress or result of business operations conducted on a large scale'.

[2.11.1.5] The exceptions to the Hearsay Rule for documents, that is, for public documents, business records and bankers' books, are all designed to assist the court in the search for truth. If such documents were excluded from evidence, except through a witness who could attest to a document's creation and authenticity, trials would undoubtedly take much

[158] Stone and Wells, above n 28.
[159] Ibid 96.
[160] (1840) 4 Jur 172; 6 M & W 5.
[161] 8 & 9 Vict c 113.
[162] (1984)1 FCR 172.
[163] (1913) 30 TLR 190.
[164] (1937) 37 SR (NSW) 314.
[165] (1940) 64 CLR 282.

longer, be more expensive and be subjected to absurd technicalities for exclusion of evidence. These exceptions to the Hearsay Rule allow relevant evidence to be considered by the courts. The question to be answered by this thesis, however, is whether those same rules should be applied to electronic documents, whether they are public, business records or bankers' books, or even if the rules should be applied but in a slightly different way.

2.12 Testamentary Evidence

[2.12.1.1] In *The Jury and the Exclusionary Rules of Evidence,*[166] Edmund M. Morgan writes:[167]

> The common law preference for the testimony of attesting witnesses likewise finds its origin in days long antedating the jury; they are the successors of 'that very ancient class of transaction or business witnesses, running far back into the old Germanic law, who were once the only sort of witnesses that could be compelled to come before a court.

[2.12.1.2] This rule was amended by *Common Law Procedure Act 1854* (Eng) s 6, and *Criminal Procedure Act 1865* (Eng) s 7, which provided: 'It shall not be necessary to prove by the attesting witness any instrument to the validity of which attestation is not requisite and such instrument may be proved as if there had been an attesting witness'.[168]

2.13 Evidence produced by machines and devices

[2.13.1.1] The *Uniform Evidence Acts* s 146 provides as follows:

> **146. Evidence produced by processes, machines and other devices**
> (1) This section applies to a document or thing:
> (a) that is produced wholly or partly by a device or process; and
> (b) that is tendered by a party who asserts that, in producing the document or thing, the device or process has produced a particular outcome.
>
> (2) If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document or thing on the occasion in question, the device or process produced that outcome.

[2.13.1.2] In summary, *Uniform Evidence Acts* s 146 creates a rebuttable presumption that, where a party tenders a document or thing that has been produced by a process or device, if the device or process is one that, if properly used, ordinarily produces a particular outcome, then in producing the document or thing on this occasion, the device or process has produced that

[166] Quoted in Gilbert, above n 110, 251.
[167] Ibid 251.
[168] *Criminal Procedure Act 1865* (Eng) s7.

outcome. For example, where a scanner has made an image copy of the document then it would not be necessary to call evidence to prove that the scanner was working properly when it was used to create an image of the document. The *Uniform Evidence Acts* s 147 provides a similar rebuttable presumption where documents are produced by processes, machines and other devices in the course of business.[169] That section provides as follows:

> **147. Documents produced by processes, machines and other devices in the course of business**
>
> (1) This section applies to a document:
>
> (a) that is produced wholly or partly by a device or process; and
>
> (b) that is tendered by a party who asserts that, in producing the document, the device or process has produced a particular outcome.
>
> (2) If:
>
> (a) the document is, or was at the time it was produced, part of the records of, or kept for the purposes of, a business (whether or not the business is still in existence); and
>
> (b) the device or process is or was at that time used for the purposes of the business;
>
> it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document on the occasion in question, the device or process produced that outcome.
>
> (3) Subsection (2) does not apply to the contents of a document that was produced:
>
> (a) for the purpose of conducting, or for or in contemplation of or in connection with, an Australian or overseas proceeding; or
>
> (b) in connection with an investigation relating or leading to a criminal proceeding.

[2.13.1.3] The presumption in *Uniform Evidence Acts* s 146 is rebutted when a party raises sufficient evidence to raise doubt about the presumption. Where evidence raises a doubt, it 'does not need to be of the same quality of the same probative strength as evidence that is required to satisfy the civil standard'.[170]

[2.13.1.4] In *Deputy Commissioner of Taxation v Liu*,[171] Gibson DCJ was satisfied that the plaintiff could rely upon not only *Evidence Act 1995* (Cth) s 146 but also *Evidence Act* 1995 (Cth) s 147. While the documents were produced for the purposes of litigation, the material under challenge, in particular, the parameters of the relevant accounting system were held to be inherently part of the business activities of the plaintiff.

[2.13.1.5] In its submission to the ALRC, the Criminal Law Committee of the Law Society of South Australia and the Legal Services Commission of South Australia also pointed out that the *Uniform Evidence Acts* have no direct equivalent of *Evidence Act 1929* (SA) s 59B. That

[169] *Evidence Act 1995* (Cth) ss 146,147.
[170] *North Sydney Leagues' Club Limited v Synergy Protection Agency Pty Limited* (2012) 83 NSWLR 710, 60 (Beazley JA, Macfarlan and Whealy JJA agreeing).
[171] 15 DCLR (NSW) 57.

section requires a court to be satisfied that there have been no alterations made to the machine, such as tampering with the hard drive of the computer. The ALRC and the other Commissions looked further at the South Australian approach and concluded that *Evidence Act 1929* (SA) s 45C allows the court to:

> (a) Rely on its own knowledge of the nature and reliability of the processes by which the reproduction was made;
> (b) Rely on the certification of someone with the knowledge and experience of these processes or who has compared the contents of both documents and found them to be identical; or
> (c) Act on any other basis it considers appropriate in the circumstances.

[2.13.1.6] Further, *Evidence Act 1929* (SA) s 59B makes a 'computer output' admissible, subject to the court being satisfied as to a number of matters, namely that:

> (a) The computer is correctly programmed and regularly used to produce output of the same kind as that tendered in evidence;
> (b) The data from which the output is produced by the computer is systematically prepared upon the basis of information that would normally be acceptable in a court of law as evidence of the statements or representations contained in or constituted by the output;
> (c) In the case of the output tendered in evidence, there is, upon the evidence before the court, no reasonable cause to suspect any departure from the system, or any error in the preparation of the data;
> (d) The computer has not, during a period extending from the time of the introduction of the data to that of the production of the output, been subject to a malfunction that might reasonably be expected to affect the accuracy of the output;
> (e) During that period there have been no alterations to the mechanism or processes of the computer that might reasonably be expected adversely to affect the accuracy of the output;
> (f) Records have been kept by a responsible person in charge of the computer of alterations to the mechanism and processes of the computer during that period; and
> (g) There is no reasonable cause to believe that the accuracy or validity of the output has been adversely affected by the use of any improper process or procedure or by inadequate safeguards in the use of the computer.

[2.13.1.7] The ALRC observed that 'ss 45C and 59B provide alternative approaches to the admissibility of computer-produced evidence that have the outward appeal of being broad and investing the court with wide judicial discretion to admit into evidence photographic, electronic and other reproductions'.[172]

[2.13.1.8] However, the ALRC commented 'that s 45C is flawed in that it relies entirely on the reliability of the 'approved process' without further, or actual, investigation into that process' and that, 's 59B is based on the *Civil Evidence Act 1968* (Eng), which was criticised by the Law Commission of England and Wales ('Law Commission') in a 1993 review of that

[172] Australian Law Reform Commission, *Uniform Evidence Law*, Report No 102 (2005) [6.22].

Act':

> [T]here is a heavy reliance on the need to prove that the document has been produced in the normal course of business and in an uninterrupted course of activity. It is at least questionable whether these requirements provide any real safeguards in relation to the reliability of the hardware or software concerned.[173]

[2.13.1.9] The ALRC examined research on the reliability of computers carried out by Dr Cameron Spenceley.[174] The Spenceley research identified a 'redundancy test' approach which operates to provide some level of verification that a failure in a computer has not occurred. The NSW DPP opposed the 'redundancy test' for a number of reasons,[175] and considered that any attempt to put in a 'redundancy mechanism' as a test, could result in these items of evidence being routinely challenged as to an assumed inaccuracy. With respect, this observation is correct. However, the ALRC considered that a 'redundancy test' offered a 'more rigorous requirement for admissibility of computer-produced material that arguably balances the need to ensure reliability of evidence with the need for an efficient practice for use in litigation'. However, it is arguable that the reliability of computers is no longer in question unless one party calls it into question and indeed, there is a presumption that mechanical instruments or technological devices function properly. In *Barker v Fauser,*[176] Travers J explained that in our ordinary experience of life, there is a general probability that instruments such as watches and weighbridges are substantially correct; also they are rarely completely accurate, they are so substantially accurate that people go on using them.[177] Courts have presumed traffic lights to be working property, stop watches, speedometers, weighing machines, although these

[173] Australian Law Reform Commission, *The Hearsay Rule in Civil Proceedings*, Report 216 (1993) [3.15].
[174] Cameron Spenceley, *Evidentiary Treatment of Computer-Produced Material: A Reliability Based Evaluation*, (PhD Thesis, University of Sydney, 2003).
[175] Ibid. The NSW DPP considered that the term 'redundancy mechanism' is not readily understood. Further, the 'redundancy test' is set at the civil standard of proof and is not relevant to criminal trials. If the verifying mechanism built into the computer system is itself either another computer or part of a computer, should the verifying mechanism also require a 'redundancy mechanism'? For example, if a customer checks a bank statement with the bank, the evidence would be hearsay and when the bank checked its own computerised record, unless the 'verifying measure' is a guarantee of accuracy (which it is not), it may merely repeat or corroborate whether problem exists in the data generation process. There would be significant compliance costs in the extra evidence required to overcome an unidentified, unquantified, assumed risk. Likewise, the cost of acquiring a 'redundancy mechanism' may put this beyond the reach of smaller litigants and thereby unfairly disadvantage them. Finally, the impact of such a test is potentially far-reaching as there are so many documents and other material, such as records, tests and photos, produced on computer or using computer technology. Any requirement that computers be subject to a 'redundancy mechanism' could result in these items of evidence being routinely challenged as to an assumed inaccuracy.
[176] (1962) SASR 176.
[177] Ibid 178-9.

presumptions can be called into question using appropriate evidence. Mason[178] provides a thorough examination of whether both computer hardware and software can be considered reliable, and this thesis asks whether new and different questions should be posed when examining whether data stored on computer systems can be authenticated.

[2.13.1.10] Reference was made, by the ALRC, to the argument of Emmanuel Laryea[179] that:

> It must be ensured … that adequate safeguards for testing computer evidence are put in place. Courts should be given, and use, wide powers to ensure that computer systems and electronic data are sufficiently tested for integrity and reliability when necessary.[180]

[2.13.1.11] However, the Commission observed that the case law dealing with *Uniform Evidence Acts* ss 146 and 147 has not indicated that there are any problems with the operation of these provisions.

[2.13.1.12] There were seven submissions to the Commissions addressing the question of the reliability of computer-produced evidence, three supported[181] a more rigorous test and four opposed it.[182] The Office of the Director of Public Prosecutions (NSW) ('the NSW DPP') opposed a higher threshold for admissibility of computer-produced documents for a number of reasons, which the Commissions summarised as follows:

> (a) There is no solid evidence that such a provision is needed and no cases of wrongful conviction from computer-generated error;
> (b) Litigation in Australia depends on an adversarial system and the burden of proof that rests on the prosecuting party, or plaintiff, ensures proper testing of evidence of this sort;
> (c) It would impose a higher threshold than for other 'machine produced evidence';
> (d) Data manipulation can occur with any machine-generated information, such as photos, tapes and videos; and
> (e) The party challenging the accuracy of the evidence would have to be given the opportunity to inspect the relevant computer and perform their own tests which would be a costly and time-consuming exercise.[183]

---

[178] Stephen Mason (ed), *Electronic Evidence* (LexisNexis Butterworths, 3rd ed, 2012) [5.01] to [5.37].
[179] Emmanuel Laryea, 'The Evidential Status of Electronic Data' (1999) 3 *National Law Review* 1 [27].
[180] Australian Law Reform Commission, *Uniform Evidence Law*, Report No 102 (2005), 170.
[181] The Law Society of South Australia, Submission E 69, 15 September 2005; Office of the Victorian Privacy Commissioner, Submission E 115, 30 September 2005; The Criminal Law Committee and the Litigation Law and Practice Committee of the Law Society of New South Wales, Submission E 103, 22 September 2005.
[182] Director of Public Prosecutions (NSW), Submission E 17, 15 February 2005; Commonwealth Director of Public Prosecutions, Submission E 108, 16 September 2005; Attorney-General's Department, Submission E 117, 5 October 2005; New South Wales Public Defenders, Submission E 89, 19 September 2005.
[183] Director of Public Prosecutions (NSW), Submission E 17, 15 February 2005.

[2.13.1.13] The Australian Government Attorney-General's Department noted that in criminal matters, the prosecution may not have much choice about the type of documentary material available to it and it is unlikely to be in the interests of justice to require a court to reject evidence that appears cogent and reliable and which can be corroborated by other evidence, simply because it does not satisfy formal preconditions for admissibility.[184]

[2.13.1.14] The Commonwealth Department of Public Prosecutions (CDPP) submitted there were actually significant benefits to be derived from the presumption of accuracy of computer output as the presumption facilitates the admissibility of the large number of documents and business records generated from computers. It questioned whether a more rigorous test should be put in place given that computer-produced evidence is becoming more pervasive.[185]

[2.13.1.15] Of those in favour of a more rigorous test, the Office of the Victorian Privacy Commissioner gave the example of speed camera evidence to indicate that technology-generated evidence has been shown to be less than reliable and to maintain public confidence in the judicial process is critical.[186] It was submitted that such technologies should be subject to scrutiny to maintain the highest standards of testing computer evidence, especially as computer systems become more sophisticated and complex.[187]

[2.13.1.16] The Law Society of New South Wales stated that 'in an age of computer hacking and viruses the rebuttable presumption in *Uniform Evidence Acts* s146 is of concern'.[188] It pointed out that *Uniform Evidence Acts* s 146 envisages application to machine-produced evidence such as photocopies but simply data copying is considerably different from computer-produced data, which can be stored and manipulated. It submitted that the existence of quality control or internal control systems should be sufficient for computer-produced evidence to be considered prima facie accurate and reliable, however, questioned what the standard of quality control should be and suggested there may have to be different standards for different litigants. It also submitted concerns about the accuracy and reliability of computer-produced evidence

[184] ALRC, above n 180,172.
[185] Ibid.
[186] Office of the Victorian Privacy Commissioner, Submission E 115, 30 September 2005.
[187] Ibid.
[188] Litigation Law and Practice Committee of the Law Society of New South Wales, Submission E 103, 22 September 2005, 173.

such as Short Message Service ('SMS').

[2.13.1.17] The ALRC concluded that a major overhaul of the legislation is 'neither warranted nor desirable'. The ALRC's view was that a persuasive case for change should exist before a legislative amendment would be recommended. The reasons for the ALRC's view was that those opposing a change highlighted the lack of evidence of problems arising from the operation of *Uniform Evidence Acts* ss 146 and 147 and a more rigorous test is not justified. Because of the lack of empirical evidence justifying a more rigorous test, the ALRC was not persuaded that a change was required.[189]

[2.13.1.18] With respect, what the ALRC failed to do was to examine the fundamental nature of computer-generated evidence compared with paper evidence and whether the existing rules that have been developed around documentary evidence, can still apply to computer-generated evidence. As mentioned above in section [2.13.1.8], Mason[190] has examined whether computer hardware and software can be assumed to be reliable, and his overall conclusion is that they cannot be, due to the number of 'bugs' often encountered in software and failures associated with hardware. However, the question for this thesis is whether, despite these many problems with computer systems, should admissibility be subject to a challenge where the challenging party can prove those 'bugs' and/or failures affected the evidence?

2.14 Signatures

[2.14.1.1] The function and purpose of a signature will generally depend upon the nature in which it is affixed to a document, although a signature is essentially used to authenticate the instrument being signed.[191] However, a signature can be for additional uses, such as 'providing for the integrity of a message or document'.[192]

[2.14.1.2] There appears to be very little judicial or academic comment that actually defines a signature,[193] and it seems to have been understood, historically, that is before the advent of an 'electronic signature', that a signature is a signatory's name written in their own

[189] Australian Law Reform Commission, *Uniform Evidence Law*, Report No 102 (2005).
[190] See Mason, above n 178.
[191] *Caton v Caton* (1867) LR 2 HL 127.
[192] Stephen Mason, *Electronic Signatures in* Law, 3rd ed, Cambridge, 2012 at 1.
[193] Sharon Christensen, Bill Duncan & Rouhshi Low, 'Moving Queensland Property Transactions to the Digital Age: Can Writing and Signature Requirements be Fulfilled Electronically?' (2002) *Centre for Commercial and Property Law, Queensland University of Technology: Brisbane* 35.

hand on a piece of paper.[194] Courts have, however, accepted a wide range of marks as signatures, for example crosses, initials, printed names and rubber stamps.[195]

[2.14.1.3] With electronic signatures, 'in an electronic environment, the original of a message is indistinguishable from a copy, bears no handwritten signature, and is not on paper'.[196] Therefore, the question is how electronic forms of signatures can be functionally equivalent to handwritten signatures and other forms of authentication methods such as seals and stamps. For the concept of functional equivalence to have any validity, the function of a signature must first be established.

[2.14.1.4] Attempts have been made to provide uniform rules on electronic signatures,[197] however, before examining these, what constitutes an electronic signature needs to be understood.

2.14.2 Types of Electronic Signatures

[2.14.2.1] The method of affixing an electronic signature can comprise many different forms, such as:

(a) A manual signature transmitted by facsimile;
(b) Typed name;
(c) Digitised picture or image of a manual signature;
(d) Alphanumeric string or asterisk;
(e) Biometrics;
(f) Digital signatures;
(g) Clicking through a series of screens to affirm intention to make an Internet purchase;
(h) Clicking on a button labelled 'I agree' or 'purchase now';
(i) Voice on an answering machine;
(j) Including your name as part of an electronic mail communication or including the firm name on a facsimile. [198]

[2.14.2.2] Each of the methods of affixing a signature mentioned above are capable of representing a valid signature, however, issues such as affirming the identity of the person who

---

[194] Ibid, citing C Reed 'What is a Signature?' 2000(3) *Journal of Information, Law and Technology* located at <http://elj.warwick.ac.uk/jilt/00-3/reed.htm> at 11 September 2015; see also Denning LJ in *Goodman v J Eban* [1954] 1 All ER 763 at 561: 'In modern English usage when a document is required to be "signed by" someone that means that he must write his name with his own hand upon it". See also Stephen Mason, *Electronic Signatures in Law* (Cambridge University Press, 3rd ed, 2012), 16 where it is noted that in England, an early record of a manuscript signature is that of Edward III of 1362, who signed a document with his name.

[195] *R v Moore Ex Parte Myers* (1884) 10 VLR 322.

[196] *United Nations Convention on the Use of Electronic Communications in International Contracts*, United Nations, New York, 2007, p52.

[197] Ibid.

[198] Christensen, Duncan & Low, above n 193, 76.

affixed the signature, ensuring the integrity of the signature and proving the reliability of the signature must be considered, in the event a signature is challenged.

[2.14.2.3] Where a handwritten signature on paper has been scanned to an image, and the image placed into a document, this can constitute an electronic signature. The file containing the scanned signature can then be attached to a document or an email.

[2.14.2.4] An electronic signature can be secure or insecure. Unless the document is encrypted in some way, the risk is that the signature has been tampered with. An electronic signature is one which affixes a form of authentication to an electronic document, while a digital signature is a specific form of electronic signature involving encryption.[199] More particularly, a digital signature is 'data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit'.[200]

[2.14.2.5] An electronic signature can be anything in electronic form that can be used to demonstrate a signing entity intended their signature to have legal effect.[201] Typing a name into a document electronically can be an acceptable signature, although it will not necessarily be accepted in all jurisdictions for all purposes.[202] Known as the 'authenticated signature fiction', it has enjoyed some success in England & Wales. For example, in *Leeman v Stocks*[203] the writing of the vendor's name in a contract by an auctioneer was considered sufficient, after the purchaser signed the same contract to constitute a signature, for the purpose of proof under the *Statute of Frauds*. However, in Australia, this doctrine has not been adopted. In *Madden v Wright*,[204] the contrary view was held in that typing the purchaser's name into a contract following an auction was not sufficient.[205]

[2.14.2.6] A person's name in an email address is capable of identifying a person, especially where an email address emanating from an organisation, public or private, is allocated by setting out the name of the person followed by the domain name of the organisation. There are other variations that can be used, such as when an email address

[199] Ibid 47.
[200] Mason, above n 192, 189.
[201] Ibid.
[202] Ibid, 190.
[203] [1951] 1 Ch 941.
[204] (1991) Q Conv R 54-586.
[205] The court has recognised that the law is unsettled in this respect: *Kation Pty Ltd v Lamru Pty Ltd* [2011] NSWSC 219 see White J at [37], *cf Stuart v Hishon* [2013] NSWSC 766.

describes the office or function of the person, rather than their name. However, even this, if allocated to a single person, can also function to identify a particular person, subject to evidence to the contrary.

[2.14.2.7] Personal identification number (PIN) and password is another form of signature which is regularly used online. Whether or not someone authorised a particular transaction using a PIN and password will be a matter of evidence. The PIN is unique and is often the subject of theft. In the majority of cases, whether a person affixed their electronic signature does not tend to be the issue. However, there are a number of disputes regarding withdrawals from bank Automatic Teller Machines ('ATMs'). If a bank issues a card with a chip, the chip contains the private key of a digital signature, with the PIN being the password. Thieves who know how to by-pass security on these cards illustrates the problem of protecting the private key with a PIN or password.[206]

[2.14.2.8] In *Shojibur Rahman v Barclays Bank PLC,*[207] the issue involved the claimant denying that he authorised debit card transactions. For electronic transactions between a bank and customer, *prima facie,* a way of authorising the identity of the customer was required, and a thief had obtained the appellant's debit card, PIN and other significant details through fraud. When authorising a purchase of a Rolex watch of significant value, the thief answered some questions correctly but others were vague. The court dismissed the customer's claim, on the basis that the customer had not sufficiently protected his PIN and other confidential information. The decision in this case has been criticised by Mason and Bohm,[208] to the extent that 'it appears clear that the bank, by its own admission, failed to authenticate the holder of the card effectively, or at all',[209] and that 'the resistance of banks to submit proper evidence with respect to unauthorised withdrawals from Automatic Teller Machine ('ATM') and online banking disputes, should be the topic of constant vigilance by lawyers and judges alike'.[210]

[2.14.2.9] There are products that permit a person to produce a biodynamic version of their

[206] See further Steven J. Murdoch, Saar Drimer, Ross Anderson and Mike Bond, 'Chip and PIN is Broken', 31st IEEE Symposium on Security and Privacy, IEEE Computer Society, 2010, pp 433-446; <http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf> as at 5 January 2016.
[207] [2014] EWCA Civ 811 (Moore-Bick LJ).
[208] Stephen Mason and Nicholas Bohm, 'Commentary on Appeal Judgment'(2013) 10 *Digital Evidence and Electronic Signature Law Review* <http://journals.sas.ac.uk/deeslr/article/view/2041/1978>.
[209] Ibid 12.
[210] Ibid 13.

manuscript signature. For instance, some delivery companies use hand-held devices that require the recipient of an item of post or parcel to sign on a screen to acknowledge receipt of the mail or parcel. Similarly, some laptop computers allow a signature to be captured using a digital pen and the laptop's trackpad. Indeed, this method of affixing a signature has been approved by the Federal Court of Australia: *Getup Ltd v Electoral Commissioner*,[211] where Perram J concluded that a signature affixed to an enrol-to-vote form using a digital pen applied to the laptop's trackpad, was sufficient for the purposes of the *Electoral Act 1918* (Cth). Further, his Honour held that the *Electronic Transactions Act 1999* (Cth) applied to enable a digital signature to give effect to the form.

[2.14.2.10] This technology allows the signature to be captured by way of a series of measurements, which record the behaviour of the person as they perform the action. The measurements can include the speed, rhythm, pattern, habit, stroke sequence and dynamics that are unique to the individual at the time they write their signature. The subsequent electronic file can then be attached to any document in electronic format to provide a measurement of a signature represented in graphic form on the screen. Whether pen pressures are stored is dependent upon both the hardware and software. The tablet must have pressure sensing hardware built into the screen and then software must specifically utilise that hardware. For example, the Microsoft Surface Pro 3 has pressure hardware built in but only some of the software programs, such as those designed for drawing (for example, Adobe Photoshop, Microsoft Paint), would make use of the pressure technology.

[2.14.2.11] For other programs, the software simply captures the line, as if the left mouse button was being dragged around the screen. With regard to the storing of information of a pen/tablet, each pen stroke has its coordinates stored (start and end points). For a straight line that is quite easy, however, for handwriting it would be broken down to all combinations of straight lines. So a single handwritten letter may have hundreds of pairs of coordinates stored. Along with the start/end coordinates of each line a pen, the pressure/density/thickness value would also be stored. Whether this combination of hardware and software could be used to verify a handwritten signature to prevent repudiation, is yet to be tested in court. However, this appears to be an area which could supersede handwritten signatures on paper and in the same way as an expertise in forensic handwriting has developed, an expertise in forensic

[211] [2010] FCA 869.

handwriting captured electronically, could develop. The difficulty lies in evidence needed to demonstrate the use that such a signature can be linked to a human being.[212]

[2.14.2.12] Biometric measurements are another form of electronic signature. These allow authentication of an individual by measuring the person's physical characteristics, such as height and weight, voice recognition, retinal scans, fingerprints, facial recognition and even DNA patterns.[213] However, as Mason notes, there are a number of difficulties in using biometric measurements including the range of tolerances to reduce false negatives, and the accuracy of the software.[214] There are difficulties in using biometric measurements, such as fingerprints, due to the number of problems associated with fingerprint scanners, including criminals forcing users to place their finger against a scanner, using artificial clones of fingerprints, to name a few.[215]

[2.14.2.13] In this day of internet transactions, clicking 'I agree' or 'I accept' can confirm an intention to enter into a contract when buying good or services online.[216] In England and Wales, the Law Commission has suggested that this form of signature is the technological equivalent of a manuscript signature.[217] Mason suggests that this analysis is sound.[218] As Mason points out, in English law, the validity of a signature depends upon the function it performs, not necessarily the form in which it takes.[219] The only issue with this form of signature, as with many types of electronic signature, is proving the identity of the person purporting to have made the signature.

[2.14.2.14] Handwritten signatures have traditionally been used as a method of authentication, and indeed the 'science' of forensic handwriting has grown out of cases where experts can determine forgeries by examining handwriting patterns. However, the equivalent process to determine the authenticity of an electronic signature is yet to be implemented, despite various electronic signature frameworks having been developed.

---

[212] See Heidi H. Harralson, 'Forensic document examination of electronically captured signatures', 9 *Digital Evidence and Electronic Signature Law Review* (2012) 67-73.
[213] Mason, above n 192, 270.
[214] Ibid.
[215] Ibid at 271 where Mason lists a number of issues with fingerprint scanners.
[216] Ibid.
[217] Mason, above n 192, 218.
[218] Ibid.
[219] Ibid.

2.14.3 Digital signatures & Public Key Infrastructure

[2.14.3.1] Digital signatures use cryptography to encrypt, and then decrypt the electronic text comprising the signature.[220] A digital signature is a unique sequence of numbers generated by an algoritm; the cryptographic application used means that any change to the text, however small, will be identified, and therefore can be used as a means of authentication. As explained by Mason,[221] there are two types of cryptographic systems: symmetric and asymmetric systems.

[2.14.3.2] A symmetric system uses the same cipher, or key, for both encryption and decryption. Ostensibly, an interceptor is unable to decrypt the message without the cipher, or key, however, there can be problems with secure transportation of the key to the recipient for decryption. Consequently, a symmetric system has difficulties when there are large number of users, due to the large number of keys required. The development of the asymmetric cryptographic system uses a public key, assists to solve this problem.[222]

[2.14.3.3] With an asymmetric cryptographic system, one key is used to encrypt the message and the other key is used to decrypt the message. The encryption key can be made public and 'anybody can use the encryption key to encrypt a plaintext message, but only the person with the decryption key, or the 'private key', that corresponds to the encryption key can decrypt the message'.[223] The weakness with the private key is that it needs to be secured, for example, by a password and passwords are notoriously problematic.[224] As Mason postulates, the problem is in how to attribute actions recorded in a digital format, to a specific human being.[225]

[2.14.3.4] Further, the public key can be stored in a public database. The problem, however, lies in ensuring that the public key belongs to the person claiming to have created it, so a Certificate Authority (CA) can be used as a 'trusted' source, that is, an entity that can be trusted to identify provider of the public key.

[2.14.3.5] The CA, in theory, guarantees the authenticity of the public key by issuing an

[220] Mason, above n 192, 259-260.
[221] Ibid at 261
[222] Ibid at 263-264.
[223] Ibid at 265-266.
[224] See further discussion Mason, above n 192, Chapter 16.
[225] Ibid.

'individual identity certificate',[226] which 'binds a name string to a public key. This in turn seeks to create a link between the provision of a key and the identity of the natural person or legal entity to which the key has been issued'.[227]

[2.14.3.6] One of the many technical problems facing PKI is that the CA itself should be verified, thereby leading to a never-ending round of cross-certification requirements. There are other concerns that the private key is subject to sabotage and therefore is insecure.[228] There appears to be a shift away from a PKI providing some 'magical solution' for security of electronic systems, and instead the focus is on providing security at an application level.

[2.14.3.7] With a digital signature, it may simply indicate that someone with access to the key has signed the document, however, keys can be stolen without the knowledge of the owner.[229] Therefore, proving that the person whose name appeared actually digitally signed the document, may require additional evidence.[230] Just as a body of law has been established for handwriting verification, so too will the law develop around digital signature. However, we are not yet at that point.

[2.14.3.8] In Australia, a 'Certification Authority' is defined as a Gatekeeper Accredited Service Provider that issues Digital Certificates that have been Digitally Signed using the Certification Authority's Private Key and provides certificate verification and revocation services for the Digital Certificates it issues. 'Gatekeeper' means the Commonwealth Government strategy to develop PKI to facilitate Government online service delivery and e-procurement. Gatekeeper Accredited Service Provider means a service provider accredited by the Gatekeeper Competent Authority. Gatekeeper Competent Authority means the entity which approves an application for Gatekeeper accreditation. The Gatekeeper Competent Authority for PKI is the Australian Government Chief Information Officer, Australian Government

[226] Ibid at 266.
[227] Ibid.
[228] Ibid and pp 309-310.
[229] See for example, where thieves obtained access to private keys and transferred money from corporate bank accounts electronically in the Russian Federation. See further Olga I. Kudryavtseva, 'The Use of Electronic Digital Signatures in Banking Relationships in the Russian Federation', 5 *Digital Evidence and Electronic Signature Law Review* (2008) 51-57; Olga I. Kudryavtseva, 'Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N KT-A 40/8531-03-IT', 5 *Digital Evidence and Electronic Signature Law Review* (2008) 149-151.
[230] The Sedona Conference, Commentary on ESI Evidence & Admissibility, March 2008, <http://www.thesedonaconference.org> at 11 September 2015, 14.

Information Management Office, Department of Finance and Deregulation.[231]

[2.14.3.9] Some Commonwealth government departments provide digital certificates to users who wish to transact with that department, and such certificates are based on the Gatekeeper (Public Key Infrastructure) framework. However, this means that a user has to obtain a new digital certificate each time it transacts with a different department or a different entity. For example, health care professionals can obtain a Medicare Public Key Infrastructure (PKI) certificate to access online services. Individuals and businesses who wish to transact with the Australian Taxation Office need an AUSkey in order to transact with the ATO. They keys are stored on a computer or even an external storage device, and require a password for authentication. Leaving aside the issue of intercepting the key, the main problem is that one person can have many different digital signatures. With handwritten signatures, each person only requires a pen to affix their signature.

2.14.4 Signatures under the Statute of Frauds

[2.14.4.1] At common law, under the *Statute of Frauds*, certain documents had to be personally signed by the party to be charged, or signed by a lawfully appointed agent of the party to be charged.[232] A signature is said to be unique to the signatory. A signature serves the following functions:

1. It identifies the signatory;
2. It evidences the party's approval of the contents of the document; and
3. It provides integrity for the contract between the parties ensuring the reliability and admissibility of the parties' agreement in court.[233] [*Emphasis added*].

[2.14.4.2] The question raised by the use of electronic documents, is whether a signature can be valid for evidentiary purposes, notwithstanding that it has been affixed electronically. The courts seem to be concerned that the requirement of a signature depends the particular method used, however, the following passage from *Goodman v J Eban*[234] by Romer LJ indicated that it is the function that the signature is intended to perform which is all important:

> The first reaction of many people, I think, would be that the impression of a name produced by a rubber stamp does not constitute a signature, and indeed, in some sense, is the antithesis of a

[231] The Australian Government Gatekeeper PKI Framework, February 2009, <http://www.finance.gov.au/files/2012/04/Gatekeeper_PKI_Framework.pdf> at 11 September 2015.
[232] Refer section [2.6.1.2] for a discussion of these.
[233] *Leeman v Stocks* (1951) Ch 941 [947]-[948].
[234] [1954] 1 All ER 763.

> signature. When, however, the matter is further considered in light of authority and also of the function which a signature is intended to perform one arrives, I think, at a different result.[235]

[2.14.4.3] Mason concludes that 'when a signature is in electronic format, more considerations will apply to the signature',[236] and highlights that a digital signature requires the following attributes:

> a. The signature must be authentic. In this respect the method ought, ideally, to provide for the authentication of the origin of the data and the integrity of the message.
> b. There ought to be a technical method in place that prevents the person appending the signature to the document from claiming later that they did not sign it. This is virtually impossible to achieve in the electronic environment. Care must be taken to distinguish between the degree of probability that a system can be designed to prevent a person from making such a claim, and any suggestion of a presumption that purports to bind the user to the signature that is verified.
> c. The signature should not be capable of being forged, in that the private key is secure.
> d. Where a signature is added to a message that comprises a legal act, the signature and its link to the relevant document should remain verifiable for as long as it is of legal importance.
> e. The signature cannot be reused.
> f. The document that has been signed cannot be altered without rendering the signature unverifiable.[237]

[2.14.4.4] As discussed in section [2.14.1.3] above, the question is how electronic forms of signatures can be functionally equivalent to handwritten signatures and other forms of authentication methods; for the concept of functional equivalence to have any validity, the function of a signature must first be established.

[2.14.4.5] In Australia, the question is whether an electronic signature is sufficient to satisfy the terms of the *Statute of Frauds* provisions. There are two legislative frameworks where an electronic signature can be accepted; one is under the various *Electronic Transactions Acts* and the other is under the *Electronic Conveyancing National Law*. Both of these frameworks are considered in sections 2.14.5 and 2.14.6 respectively

2.14.5 Signatures under the Electronic Transactions Acts

[2.14.5.1] The *Electronic Transactions Act 1999* (Cth) ensures that a transaction under a Commonwealth law will not be invalid simply because it was conducted through electronic communication. Each state and territory has its own Electronic Transactions

[235] Ibid 557.
[236] Mason, above n 192, 267
[237] Ibid at 267-268

Act,[238] (‘*Electronic Transaction Acts*’), each of which are similar to, but not identical, to the *Electronic Transactions Act 1999* (Cth). The principles underlying the legislation are ‘functional equivalence’, that is, no discrimination will be made between paper based transactions and electronic transactions, and that a contract that is formed automatically is not invalid, void or unenforceable because there was no human review or intervention.[239]

[2.14.5.2] The *Electronic Transactions Acts* were the result of the work of the Electronic Commerce Expert Group, which envisaged a framework for electronic commerce legislation ‘by which all other laws in Australia will be interpreted’.[240] The legislation is part of the government's ‘strategic framework for the development of the information economy in Australia’ and is based on the *United Nations Commission on International Trade Law (UNCITRAL) Model Law On Electronic Commerce of 1996*,[241] with some modifications.

[2.14.5.3] In today’s digital age, documents are commonly ‘signed’ in electronic format. The *Electronic Transactions Acts* were enacted to ensure that such commercial transactions are not invalid because they took place by means of one or more electronic communications.[242] The effect of the *Electronic Transactions Acts* is that electronic forms of documents and any ‘signatures’ that appear on such documents, are valid as long as certain conditions are met.

[2.14.5.4] The *Electronic Transactions Acts* provide that if an organisation is to retain a document (see below for an explanation of ‘document’ in relation to data) in electronic form then the integrity of the process to generate the electronic document must be assured, the information in the document must be readily accessible; and data storage requirements must be adequate. *Electronic Transactions Act 1999* (Cth) s 10(1)[243] provides that if a signature of a

---

[238] *Electronic Transactions Act 2000* (NSW), *Electronic Transactions Act 2000* (Vic), *Electronic Transactions Act 2001* (Qld), *Electronic Transactions Act 2000* (SA), *Electronic Transactions Act 2011* (WA), *Electronic Transactions Act 2000* (Tas), *Electronic Transactions Act 2001* (ACT), *Electronic Transactions Act* (NT).

[239] *Electronic Transactions Act 1999* (Cth), s 15C*; Electronic Transactions Act 2000* (NSW), s 14C; *Electronic Transactions (Victoria) Act 2000* (Vic), s 14C; *Electronic Transactions (Queensland) Act 2000* (Qld), s 26C; *Electronic Transactions Act 2000* (SA), s 14C; *Electronic Transactions Act 2011* (WA), s 19; *Electronic Transactions Act 2000* (Tas), s 12C; *Electronic Transactions Act 2001* (ACT), s 14C; *Electronic Transactions (Northern Territory) Act* (NT), s 14C.

[240] Aaron Upcroft, ‘E-Commerce Global or Local? An Australian Case Study’ (1999) 10(1) *Journal of Law, Information and Science* 113.

[241] *Model Law on Electronic Commerce*, (1996) UNCITRAL: <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html> at 11 September 2015.

[242] *Electronic Transactions Act 2000* (NSW) ss 4(a), 7(1).

[243] *Electronic Transactions Act 2000* (NSW) s 9(1), *Electronic Transactions Act 2000* (Vic) s 9(1), *Electronic Transactions Act 2001* (Qld) s 14(1), *Electronic Transactions Act 2000* (SA) s 9(1), *Electronic Transactions Act*

person is required, the requirement is taken to have been met in relation to an electronic communication if:

> (a) in all cases--a method is used to identify the person and to indicate the person's intention in respect of the information communicated; and
> (b) in all cases--the method used was either:
> (i) as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
> (ii) proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence; and
> (c) if the signature is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the method used as mentioned in paragraph (a) be in accordance with particular information technology requirements--the entity's requirement has been met; and
> (d) if the signature is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity--the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned in paragraph (a). *Emphasis added.*

[2.14.5.5] Some commentators[244] suggest that the *Electronic Transactions Acts* may not provide adequate protection for parties in land transactions and suggest that only a two-tiered structure such as that outlined in the UNCITRAL model law on electronic commerce will suffice. The difficulties of guaranteeing the identity of the signatory have been identified above and therefore an electronic signature, unless coupled with some means of verifying the signature, may fall short of the *Electronic Transactions Acts* requirements. This may certainly be the case for land contracts where, as much as it is possible, there must be an absolute guarantee against fraud, and the *Statute of Frauds* provisions which are reflected in modern legislation, may mean that an electronic signature may not be valid for land contracts, contracts for guarantees, insurance contracts and for assignments of intellectual property. However, the *Electronic Conveyancing National Law* does allow electronic signatures to be accepted, under the terms set out in that legislation. This is examined further in section 2.14.6 below.

2.14.6 Signatures under the Electronic Conveyancing National Law in Australia

[2.14.6.1] A *National Electronic Conveyancing System* ('NECS') was an initiative of the Council of Australian Governments (COAG) to provide a single national electronic conveyancing system for use throughout Australia.[245] In 2011, the Australian Registrars'

2011 (WA) s 10(1), *Electronic Transactions Act 2000* (Tas) s 7(1), *Electronic Transactions Act 2001* (ACT) s 9(1), *Electronic Transactions Act* (NT) s 9(1).

[244] Christensen, Duncan & Low, above n 193.

[245] Australian Registrars' National Electronic Conveyancing Council (ARNECC) website: <http://www.arnecc.gov.au/> at 11 September 2015.

National Electronic Conveyancing Council (ARNECC) was formed under the Inter-Governmental Agreement for an Electronic Conveyancing National Law (IGA) to co-ordinate a national approach among States and Territories to regulate an electronic environment for completing conveyancing transactions.[246] ARNECC was created to ensure a consistent national approach to the regulation of National E-Conveyancing.[247]

[2.14.6.2] The *Electronic Conveyancing National Law* (ECNL), which has so far been enacted by New South Wales,[248] Victoria,[249] Queensland[250], South Australia,[251] Tasmania,[252] and Western Australia,[253] will allow digital signatures to be affixed to certain documents, such as lawyers signing transfers for their clients. Otherwise, it is still necessary for the parties to the transaction to sign the hard copy. The ENCL is referred to in each State Act, either as an Appendix, Schedule or by way of re-statement.[254]

[2.14.6.3] Where clients have authorised their lawyers to sign documents, a hard copy will no longer be required for the transfer of land, a mortgage or release of mortgage. Instead, data can be provided electronically to the relevant land registry. 'Document' is defined in the ECNL as 'any record of information that exists in a digital form and is capable of being reproduced, transmitted, stored and duplicated by electronic means'.

[2.14.6.4] In order to sign transactions electronically, a lawyer must first obtain a client authorisation,[255] this authorisation allows a lawyer to 'sign' electronic documents for registration and to authorise the financial transaction. The rules surrounding these types of transactions are governed by the Model Participation Rules[256] ('MPR') developed pursuant to

[246] Ibid.
[247] Ibid.
[248] *Electronic Conveyancing (Adoption of National Law) Act 2013* (NSW).
[249] *Electronic Conveyancing (Adoption of National Law) Act 2013* (Vic).
[250] *Electronic Conveyancing National Law Act 2013* (Qld).
[251] *Electronic Conveyancing National Law Act 2013* (SA).
[252] *Electronic Conveyancing (Adoption of National Law) Act 2013* (Tas).
[253] *Electronic Conveyancing Act 2014* (WA).
[254] *Electronic Conveyancing (Adoption of National Law) Act 2013* (NSW) Appendix; *Electronic Conveyancing (Adoption of National Law) Act 2013* (Vic) Appendix contained within Endnotes; *Electronic Conveyancing National Law Act 2013* (Qld) s 4 states that the Appendix to the NSW Act is to apply; *Electronic Conveyancing National Law Act 2013* (SA) Schedule 1; *Electronic Conveyancing (Adoption of National Law) Act* 2013 (Tas) s 4 states that the Appendix to the NSW Act is to apply; *Electronic Conveyancing Act 2014* (WA) ss 7 to 94 restates the provisions of the ECNL.
[255] ENCL s 10.
[256] NSW Registrar General, *ARNECC Model Participation Rules*, version 2, 18 March 2014.

the ECNL.

[2.14.6.5] The client authorisation is not a power of attorney and only has effect for the purposes specified in the ECNL. The lawyer should check that all parts of the client authorisation are completed and that the lawyer has taken reasonable steps to (a) establish that the client is entitled to be entered into the conveyancing transaction[257] and to (b) verify the identity of the client.[258] A person who has been designated as a 'signer' by the relevant subscriber may sign electronic documents digitally. A subscriber should designate at least one person to act as a signer within the system and a subscriber is required to have at least one digital signature certificate that uses public/private key technology. It is only subscribers to the system who can access the system and sign documents. Once a subscriber has signed an electronic instruction, the ECNL deems it to (a) be in writing for the purposes of every other law of the jurisdiction[259] and (b) satisfy other laws of the jurisdiction related to execution, signing, witnessing, attestation or sealing of documents. Therefore, in an electronic system there will be no requirements for witnessing,[260] nor will the instrument need to be signed by the subscriber's client where the subscriber is acting under the client authorisation agreement or by the subscriber in all other cases.[261]

[2.14.6.6] Schedule 3 of the Model Participation Rules sets out the certifications which the signer makes, and these certifications relate to verifying identity, client authorisation, supporting evidence, that the information in the document is correct and that any duplicate certificate of title is destroyed or retrieved.

[2.14.6.7] ECNL s 12 provides that a subscriber will be bound by the use of their digital signature unless the subscriber can repudiate the signature in accordance with that section. The following rules apply regardless of who created the digital signature of the subscriber and the circumstances of its creation:[262]

> (a) the document is deemed to be signed by the subscriber;
> (b) the signature is binding on the subscriber and any other person who the subscriber is acting for under a client authorisation; and
> (c) the signature may be relied upon as the signature of the subscriber by each party to the

[257] Ibid r 6.4.
[258] Ibid r 6.5.
[259] ENCL s 9(3).
[260] Ibid.
[261] ENCL s 9(2).
[262] ENCL s 12(1)

> transaction, each subscriber acting under a client authorisation, any person claiming under or through any party to the transaction and the registrar once the document is lodged.

[2.14.6.8] This section provides for the 'attribution rule'. The only exception is when the subscriber repudiates the signature, which can be done if the requirements of the ECNL s 12(4) are met:

> (a) the digital signature was not created by the subscriber; and
> (b) the digital signature was not created by an employee, agent, contractor or officer of the subscriber who at the time had the subscriber's express or implied authority to create the signature; and
> (c) the creation of the signature was not enabled by a failure of the subscriber or their agents, employees, officers or contractors to comply with the requirements of the participation rules or a failure to take reasonable care.

[2.14.6.9] Christensen[263] notes that the attribution rule has been criticised by a number of stakeholders as resulting in liability for a subscriber in the event of fraud by an employee or a third party who obtains the ability to sign as a result of the negligence of an employee. Christensen notes that 'these observations are accurate, but the opposing view is that such attribution is necessary to ensure the integrity of the system. It means that a subscriber must maintain the security of their digital key by ensuring proper security for their own computing systems and protocols for employees authorised to sign on their behalf.'[264]

[2.14.6.10] The ECNL, while taking electronic conveyancing to the next level, still does not allow for the end client to sign their own documents. Why is this and how does a digital signature framework work? A solution may lie in examining the way in which notaries sign documents electronically in other jurisdictions.[265]

[2.14.6.11] The ECNL defines a 'digital signature' as an encrypted electronic data intended for the exclusive use of a particular person as a means of identifying that person as the sender of an electronic communication or the signer of a document.

[2.14.6.12] Model Participation Rules, r 7.5 provides that electronic documents that are to be lodged through the Electronic Lodgement Network must be digitally signed where the

---

[263] Sharon Christensen, 'A National Law for Electronic Conveyancing - New Rules and Practices for Queensland' *Thompson Reuters Online Insider* (24 May 2013) <http://blog.thomsonreuters.com.au/2013/05/a-national-law-for-electronic-conveyancing-new-rules-and-practices-for-queensland/> at 20 November 2014

[264] Ibid.

[265] Timothy S. Reiniger and Philip M. Marston, 'The Deed is Done: On-line Notarization Becomes a Reality', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 144-146.

electronic document requires a digital signature using a private key to create the digital signature. Model Participation Rules defines a 'Digital Certificate' is defined to mean 'an electronic certificate Digitally Signed by the Certification Authority which:

> (a) Identifies either a Key Holder and/or the business entity that he/she represents; or a device or application owned, operated or controlled by the business entity; and
> (b) Binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair; and
> (c) Contains the specification of the fields to be included in a Digital Certificate and the contents of each.'

[2.14.6.13] In summary, the provisions of the ECNL is the first step in the direction of allowing documents for the sale or disposition of land, in other words, documents under the *Statute of Frauds*, to be signed electronically, and to be authenticated at law. Up until the enactment of that legislation, and despite the enactment of the *Electronic Transactions Acts*, the standard practice has been that land contracts were signed in hard copy. Indeed, the parties to the agreement must still sign the contract in hard copy until such time as the ECNL can accept some form of properly authenticated electronic signature. The ENCL is the first step towards allowing documents for a disposition of an interest in land to be signed digitally. However, at the moment, the ENCL only allows for solicitors to sign, and a means of allowing end users to sign is yet to take place.

2.15 Statutory Provisions for Documentary Evidence

[2.15.1.1] The rules of evidence within Australia are now enshrined in legislation[266] and of these, the Commonwealth, New South Wales, Victoria, Tasmania, the Australian Capital Territory and the Northern Territory have uniform legislation.

[2.15.1.2] In understanding the purpose of the existing statutory definitions of documentary evidence, it is illustrative to look at the history of these statutory provisions, as they developed at common law over several centuries. The rules of evidence began to be codified by legislation early in the 20th Century, and since then, have seen several amendments between their initial enactment and the relevant Evidence Act as it stands today. There were a variety of attempts at piecemeal legislative reform before the uniform evidence legislation was

[266] *Evidence Act 1995* (Cth), *Evidence Act 1995* (NSW), *Evidence Act 2008* (Vic), *Evidence Act 2001* (Tas), *Evidence Act 1977* (Qld), *Evidence Act 1906* (WA), *Evidence Act 1929* (SA), *Evidence (National Uniform Evidence Legislation) Act 2011* (NT) and *Evidence Act 2011* (ACT).

enacted.[267] It is appropriate to review some of this history to understand the variations in approach nationally at present.

2.15.2 Commonwealth amendments

[2.15.2.1] In 1905, the Commonwealth introduced the *Evidence Act 1905* (Cth) that embodied provisions for submitting certain documents into evidence. Those documents included orders or regulations by the Governor-General, documents or books of the Commonwealth of a public nature, and documents from Parliamentary proceedings. The *Evidence (Amendment) Act 1934* (Cth) inserted a provision[268] that the production of a document purporting to be proof published by a statistician containing statistics pursuant to the *Census and Statistics Act 1905* (Cth) shall be considered evidence of those statistics. Amendments in 1963 (proof of proceedings in Parliament),[269] 1964,[270] 1973[271] and 1974[272] were all amendments concerned with public documents while the 1978 amendment[273] introduced a section concerned with the admissibility of business records as evidence. The 1978 amendment also provided a definition of 'document'.

2.15.3 Other States

[2.15.3.1] In New South Wales, *Evidence Act 1898* (NSW) ss 44 and 45 preserved the bankers' books exception to the Hearsay Rule, as long as it could be proved the books were ordinary books of the bank and the entry was made in the usual and ordinary course of business. Amendments to the *Evidence Act1898* (NSW) in 1922[274] and 1940[275] did not affect documentary evidence. However, in 1954, an amendment to s 14B(1) of the *Evidence Act 1898* (NSW)[276] provided that:[277]

> In any civil proceedings without a jury where direct oral evidence of a fact would be admissible, any statement made by a person in a document and tending to establish that fact shall, on production of the original document, be admissible as evidence of that fact if the following

[267] The Honourable J White, *Overview of the Evidence Act* (30 October 2010) Supreme Court of NSW <http://www.supremecourt.justice.nsw.gov.au/Documents/white301010.pdf> at 11 September 2015, 4.
[268] *Evidence Act 1905* (Cth), as inserted by *Evidence (Amendment) Act 1934* (Cth) sch 1 item 1.
[269] *Evidence (Amendment) Act 1963* (Cth).
[270] *Evidence (Amendment) Act 1964* (Cth).
[271] *Evidence (Amendment) Act 1973* (Cth).
[272] *Evidence (Amendment) Act 1974* (Cth).
[273] *Evidence (Amendment) Act 1978* (Cth).
[274] *Evidence Act 1898* (NSW), as amended by *Evidence (Amendment) Act 1922* (NSW) sch 1 item 1.
[275] *Evidence Act 1898* (NSW), as amended by *Evidence (Amendment) Act1940* (NSW) sch 1 item 1.
[276] *Evidence Act 1898* (NSW) s 14B(1), as amended by *Evidence (Amendment Act) 1954* (NSW) sch 1 item 1.
[277] *Evidence Act 1898* (NSW) s 14B(1), as amended by *Evidence (Amendment Act) 1954* (NSW) s 2.

> conditions are satisfied, that is to say:
> (i) if the maker of the statement either:
> (a) had personal knowledge of the matters dealt with by the statement or
> (b) where the document in question is or forms part of a record purporting to be a continuous record, made the statement (in so far as the matters dealt with thereby are not within his personal knowledge) in the performance of a duty to record information supplied to him by a person who had, or might reasonably supposed to have, personal knowledge of those matters; and
> (ii) if the maker of the statement is called as a witness in the proceedings.

[2.15.3.2] *Evidence Act 1898* (NSW) s 14B(2)(b) dealt with destruction of originals and s 43C provided for prints from photographic film where records are destroyed, but the film is preserved.[278] 'Photographic film' was defined to include any photographic plate, micro photographic film or photostatic negative. An amendment in 1966[279] inserted a new s14CB allowing business records to be tendered in criminal proceedings.

[2.15.3.3] The *Evidence (Reproduction) Act 1967* (NSW) provided, in certain cases, the period for which documents are required by law to be preserved; for this and other purposes to facilitate the production to a court, and the use in evidence, of reproductions of documents; and for purposes connected therewith. An amendment contained in the *Foreign Proceedings (Prohibition of Certain Evidence) Amendment Act 1976* (NSW) amended the *Evidence Act 1898* (NSW)[280] to make business records admissible as evidence in all proceedings and an amendment in 1978[281] inserted a provision regarding business records and bankers' books. In 1979,[282] the Act was amended in relation to Crown privilege. Furthermore, in 1986[283] the Act was further amended to cover disputed writing or signatures.

[2.15.3.4] In Victoria, Part II of the *Evidence Act1890* (Vic) pertained to Proof of Documents, division 1 referred to documents generally (mostly public documents), division 2 referred to bankers' books, division 3 referred to by-laws. An amendment in 1915 referred to proof of documents and facts by documents- includes a section on bankers' books.[284] In 1958 a new definition of 'document' was included which provided that a 'document includes any book plan paper parchment or other material whatever on which is any writing or printing or which is marked with any letters or marks denoting words or any other signs capable of carrying

[278] *Evidence Act 1898* (NSW) s 43C.
[279] *Evidence Act 1898* (NSW), as inserted by *Evidence (Amendment) Act 1966* (NSW) Sch 1 Item 1.
[280] *Evidence Act 1898* (NSW), as amended by *Evidence (Amendment) Act 1976* (NSW) Sch 1 Item 1.
[281] *Evidence Act 1898* (NSW), as amended by *Evidence (Amendment) Act 1978* (NSW) Sch 1 Item 1.
[282] *Evidence Act 1898* (NSW), as amended by *Evidence (Amendment) Act 1979* (NSW) Sch 1 Item 1.
[283] *Evidence Act 1898* (NSW), as amended by *Evidence (Amendment) Act 1986* (NSW) Sch 1 Item 1.
[284] *Evidence Act1890* (Vic), as amended by *Evidence (Amendment) Act 1915* (Vic) Sch 1 Item 1.

a definite meaning to persons conversant with them'.[285] In 1965 an amendment was made specifically dealing with bankers books[286] and in 1971, an amendment specifically to do with documents, defined very broadly, includes business records and reference to documents produced by a computer, book account, was made.[287] In 1985 an amendment dealt with certified copies of certain maps and documents to be prima facie evidence and certified copies of books of account to be treated as originals.[288]

[2.15.3.5] The Hearsay Rule was developed so out of court statements were not relied upon in seeking the truth in a matter before the courts. When considering documents, the exceptions to the Hearsay Rule were developed so that documents created by officers within organisations were not excluded in that search for truth. These documents now include public documents, business records and bankers' books, and if such documents were excluded from evidence except through a witness who could attest to a document's creation and authenticity, trials would undoubtedly take much longer and be subjected to absurd technicalities for exclusion of evidence. The question is whether these rules should continue to be applied in the same way to electronic documents.

2.16 Summary & Conclusion

[2.16.1.1] Following a review of the history of documentary evidence, it is apparent that the existing rules of evidence were developed around paper documents. Although, *prima facie*, the definition of document within the *Uniform Evidence Acts* is broad enough to cover electronic documents, it appears that electronic documents routinely admitted into evidence may be capable of challenge on the grounds of lack of authenticity. It is clear that the jurisprudential basis of the admission of electronic documents is uncertain and lacking consistency. This will be demonstrated in the next chapter which examines the various types of electronic evidence and their unique nature. Once the nature of electronic evidence has been identified and examined, the way in which present rules of evidence have been applied to electronic evidence need to be reviewed.

[2.16.1.2] One issue that the analysis in Chapter 2 highlights is that of electronic

[285] *Evidence Act1890* (Vic), as amended by *Evidence (Amendment) Act 1958* (Vic) Sch 1 Item 1.
[286] *Evidence Act1890* (Vic), as amended by *Evidence (Amendment) Act 1965* (Vic) Sch 1 Item 1.
[287] *Evidence Act1890* (Vic), as amended by *Evidence (Amendment) Act 1971* (Vic) Sch 1 Item 1.
[288] *Evidence Act1890* (Vic), as amended by *Evidence (Amendment) Act 1985* (Vic) Sch 1 Item 1.

signatures. For centuries, the most recognised form of signature has been that of a handwritten signature on paper, with some notable exceptions. Electronic signatures come in varying forms, however, it appears that the only way in which an electronic signature can be verified is if it is encrypted using a digital signature as part of a Public Key Infrastructure. Legislation, such as the *Electronic Transactions Acts*, assist to make electronic transactions enforceable, but a question mark remains over whether digital signatures can yet replace handwritten signatures for contracts for the disposition of an interest in land, for example, Therefore, the question that Chapter 2 raises is as follows:

Question 1:
Are the laws recognising electronic signatures adequate for evidentiary purposes for documents?

3. CHAPTER 3 – UNIQUE CHARACTERISTICS OF ELECTRONIC EVIDENCE

3.1 Introduction

[3.1.1.1] There are vast differences between paper evidence and electronic evidence, and to highlight these differences, it is essential to understand how electronic evidence is created and stored and ultimately retrieved for later use. These differences are of import when examining how the rules of evidence have been, and should be, applied to electronic evidence. As Judge David Harvey notes, an electronic file does not exist in itself, in that it does not exist independently from the process in which it was created.[289]

3.2 Unique characteristics of electronic documentary evidence

[3.2.1.1] Electronic evidence, compared with paper evidence, is unique.[290] It is comprised of three elements, namely (a) the storage medium upon which data is stored as binary code, (b) software which is used to interpret the binary code and (c) the content. [291] While paper has been used for centuries, storage medium and software have only recently been used to create and store documentary evidence. Before an analysis can be undertaken of the law applicable to electronic evidence, the unique properties of electronic files, and their many variations, need to be understood.

[3.2.1.2] The content which comprises electronic evidence can be generated in one of three ways: (a) content generated by humans (note issues as to authorship where there may be more than one author); generally, this evidence would be hearsay without evidence from persons who inputted the data; (b) records generated by computers only; this would be real evidence;[292] and (c) records comprising a mix of computer generated information and human input e.g. spreadsheets, which can include calculations or simulations.[293]

[3.2.1.3] As Spencely notes: 'a computer is a combination of two elements: hardware and

[289] Judge David Harvey, *Collisions in the Digital Paradigm: Legal Rules and New Technologies*, 3rd Annual New Zealand Law & Technology Conference, 18 March 2015.
[290] In *Innovative Health Group Inc. v Calgary Health Region* 2008 ABCA 219 (CanLII), Conrad JA noted that '[a] computer hard drive is a computer disc, with a large storage capacity, upon which information is stored. It is, however, a mixed storage facility that contains such things as program files, metadata, and enabling software that allows the computer to run and to interpret the encoded data', [33].
[291] Also called *Input Information* as discussed by Spenceley, above n 174, 9.
[292] Ibid.
[293] *Elf Caledonia Ltd v London Bridge Engineering Ltd* [1997] ScotCS 1, 899.

software. A reference to the operation of a computer is in reality a reference to the operation of these two components.'[294]

3.3 Differences between electronic evidence and paper evidence

[3.3.1.1] The main difference between paper evidence and electronic evidence is that the latter is digital. Many forms of digital evidence is created on a computer system. The main components of a computer system include hardware and software. Hardware includes the physical components such as the hard disk drive, the keyboard and mouse, the display system and so on. The computer also contains a processor, or central processing unit which contains a number of electrical circuits on silicon chips. Further, the computer will contain a storage device, onto which binary data is written and stored, with storage governed by random access memory (RAM), or similar.

[3.3.1.2] Software on computer systems is broken down into operating software and application software. Operating software is the software that essentially runs the computer, commonly known as the operating system. This includes software such as Microsoft Windows, Apple Macintosh and Linux. Application software is software that allows the user to create content, which in turn, is saved onto the computer's hard drive. Such application software can include Microsoft Office applications (Word, Excel, PowerPoint, Outlook etc).

[3.3.1.3] Some working groups have spent some time defining the main differences between paper and electronic documents, a more prominent group being The Sedona Conference Working Group on Best Practices for Electronic Document Retention and Production[295] ('the Sedona Conference').

[3.3.1.4] The Sedona Conference was founded in 1997 by Richard G. Braman as a non-profit, research and educational institute 'dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation and intellectual property rights'.[296] The Sedona Conference has had several working groups dedicated to the development of guidelines and standards including Electronic Document Retention and Production and International Electronic Information Management, Discovery and Disclosure, and has numerous

[294] Spenceley, above n 174, 122.
[295] The Sedona Conference, Electronic Document Retention and Production, Working Group 1 (2002).
[296] The Sedona Conference website: <http://thesedonaconference.org/> at 17 August 2015.

publications resulting from the work of those working groups.[297]

[3.3.1.5] The Sedona Conference suggests that the main differences between paper and electronic documents can be broadly grouped into six categories: (a) metadata, (b) volume and duplicability, (c) persistence, (d) dynamic, changeable content, (e) environment dependence and obsolescence and (f) dispersion and searchability.[298]

3.3.2 Metadata

[3.3.2.1] As described in section 1.3 above, metadata is electronic information about other electronic data and is created by and embedded that includes descriptive data, which points to the identification, origin or history of the file itself and relevant dates. Metadata is often not visible on a print out of the document.[299]

[3.3.2.2] Metadata is a key feature that sets electronic documents apart from paper documents. Electronic documents contain information about the file, which is recorded by the computer to assist in storing and retrieving the file. Metadata is used by the file system for system administration tasks, and for the generation, handling, transfer and storage of data within the system.[300] This metadata can contain a plethora of information about the document itself, which would not be visible if the document is printed out.

[3.3.2.3] The recent furore over the Attorney-General's perceived failure to adequately explain what metadata the government is planning to access from telecommunications providers in a bid to counter terrorism,[301] is an example of how many people, not just lawyers, misunderstand the nature of metadata. What the Attorney-General should have made clear is that it is the Internet Protocol ('IP') addresses of web sites that proposed to be collected. Therefore, if a law enforcement agency was able to collect the web site that a user visited (which is stored in the metadata), then it could determine which site the user visited. None of

---

[297] Refer to The Sedona Conference website for a list of publications: <https://thesedonaconference.org/publications/> at 17 August 2015.

[298] The Sedona Principles Best Practices Recommendations and Principles Addressing Electronic Document Production (2nd ed: 2007), <http://www.thesedonaconference.org> at 11 September 2015.

[299] *Jarra Creek Central Packing Shed Pty Ltd v Amcor Limited* [2006] FCA 1802 at [11] (Tamberlin J).

[300] The Sedona Principles Best Practices Recommendations and Principles Addressing Electronic Document Production, above n 295, 3.

[301] Ben Grubb, 'George Brandis in "car crash" interview over controversial data retention regime', *The Sydney Morning Herald* (online) 7 August 2014, <http://www.smh.com.au/digital-life/digital-life-news/george-brandis-in-car-crash-interview-over-controversial-data-retention-regime-20140806-101849.html> at 11 September 2015.

the browsing history is stored, that is, the various web pages that the user might visit from the web site's 'home' page. The metadata kept would also allow the law enforcement agency to determine the duration of time a user spent on the sites, the date they visited them, and the location of the device they visited the sites on. In some instances, one IP address may also service hundreds of different websites, so a complete list of exactly what sites were visited would not be available.

[3.3.2.4] In email, metadata will capture essential date records such as Date Sent, Date Received, Date Replied To, Date Forwarded, as well as other metadata such as To, From, CC, BCC, Sender, Subject and so on. Documents generated by specific applications, such as Microsoft Office, also contain their own metadata. In *Armstrong v Executive Office of the President,*[302] the United States Court of Appeals, District of Columbia, held that electronic records were records of the federal government and needed to be preserved as such. The court examined the differences between paper records and electronic records, and concluded that the electronic record, particularly email, contained important information, such as who sent and received the document, that was not present in the paper copy. The court said that 'without the missing information, the paper print-outs - akin to traditional memoranda with the "to" and "from" cut off and even the "received" stamp pruned away - are dismembered documents indeed'.[303]

[3.3.2.5] Collecting and analysing metadata during discovery can yield useful evidence. However, care must be taken with metadata as it can be ambiguous or even incorrect. For example, the true author of a document may be someone using a computer which was logged into by someone else. In that case, the author stated in the metadata of the document will not be the actual author of the document.[304] Dates within the metadata may also be changed if files are moved from one directory to another. Accordingly, understanding when metadata needs to be preserved is a challenge for electronic document review and production.[305]

[3.3.2.6] In *Otkritie International Investment Management Ltd &Ors v Urumov & Ors,*[306] metadata was examined as a factor for undermining the defendant's claims. The court relied

[302] 1 F.3d 1274 (D.C. Circuit Court of Appeals 1993).
[303] Ibid at [31].
[304] Ibid.
[305] Ibid.
[306] [2014] EWHC 191 (Comm) (Eder J).

heavily on the metadata such as the creation dates, authors and signature stamps of the electronic documents. The metadata indicates creation dates and signature stamps that were boldly inconsistent with Mr Pinaev's, the defendants, statements. The court held that the manipulation of the electronic evidence portrays an overwhelming likelihood that it was done or procured by Mr Pinaev.

[3.3.2.7] In summary, metadata is an integral part of any electronic document. The question for this thesis is whether the current rules acknowledge that metadata does comprise part of an electronic document and whether the courts take this into account when considering electronic evidence.

3.3.3 Volume and Duplicability

[3.3.3.1] The Sedona Conference[307] not only referred to the volume of electronic information, but called it 'the rise of crushing volumes of information in the digital realm.[308] Often, the volume of electronic documents, in comparison to hard copy documents, is much greater. Indeed, as the cost of electronic storage devices continues to decrease, it has become much easier for organisations and individuals alike to simply store everything instead of adhering to confusing and time consuming document deletion policies. The fact that electronic documents are stored in many different locations[309] also adds to the fact that it may be difficult to destroy all copies of documents.

[3.3.3.2] Email is perhaps the best example of how electronic documents are quickly created and replicated. An email will often be sent to more than one recipient, who in turn may forward on the email. The email software used to create and transmit the email automatically creates a copy of the emails as they are sent and resent. Web pages are another example of electronic documents that are created and replicated. Web pages can be automatically saved as cached files so there will be multiple copies of web pages on a system. Additionally, most systems are backed up on a daily basis, so copies of all files on the system at the time of backup will be duplicated on the backup system.[310] Electronic documents can be, therefore, present in a number of disparate locations on a number of different media due to copies being made upon

[307] The Sedona Conference, '*Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*' (December 2013) <https://thesedonaconference.org/publications> at 17 August 2015.
[308] Ibid 11.
[309] Ibid 2-5.
[310] Ibid 5.

creation, transmission, replication, backup and archival. It is unsurprising that discovery results in large volumes of documents to be reviewed.[311] Some of these locations may not even be known to the originator or initial recipient of the email.

[3.3.3.3] Duplicates are able to be identified using hash algorithms, which assign a 'digital fingerprint' to each document. Identical documents will have the same hash algorithm and can be identified as duplicates accordingly. Examples of hash algorithms are 'MD5'[312] and 'SHA-1'.[313]

[3.3.3.4] The fact that electronic documents are capable of being reproduced in an identical fashion does pose the question as to whether the concept of the original document rule is now redundant. Although this rule has been abolished in the *Uniform Evidence Acts*, it does still exist in some jurisdictions, such as Canada, and without a legislative acknowledgement about the true nature of electronic documents, courts may not be alerted to the need to consider that electronic documents can indeed by identical.

3.3.4 Persistence

[3.3.4.1] Electronic documents are more difficult to dispose of than paper documents. Paper can be destroyed by shredding or burning, whereas it is much more difficult to destroy electronic documents, as it is not simply a question of deleting the data on the computer's hard drive. Whenever a file is stored on a computer system, the computer keeps an index of the location of the files on the file storage system such that, when a user retrieves the file, the computer looks up the location of the file in the index, and knows from which sector on the hard drive from which to obtain the file. When a user 'deletes' the file, the computer system

[311] Ibid.

[312] MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321 (The IETF (Internet Engineering Task Force) is the body that defines standard Internet operating protocols such as TCP/IP; IETF Website: <http://www.ietf.org/> as at 11 September 2015). In an MD5 cryptographic hash sum, a 128-bit (16-byte) hash value is produced, typically expressed in text format as a 32 digit hexadecimal number. This is approximately 340 billion billion billion billion probable unique numbers. This enables the duplicate's authenticity to be equated with the original.

[313] SHA-1 is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology & Department of Commerce United States of America, '*Secure Hash Standard*', Computer Security Resource Centre, March 2012 <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf> at 20 November 2014. SHA-1 produces a 160-bit (20-byte) hash value. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long.

removes the file reference from the index. Therefore, if the user then tries to retrieve the file, the computer has no reference for the files and is unable to retrieve it. This means that the data for that file still resides on the hard drive of the computer system, and the space that the file occupied is simply now available to be overwritten by other data. Therefore, 'deleted' data is still able to be retrieved by a computer forensics expert. Consequently, electronic data may be recoverable long after it has been thought 'deleted'.[314]

[3.3.4.2] The only way to effectively destroy electronic evidence is through overwriting, physical destruction, applying heat or by magnetic destruction. Simply re-formatting a hard drive does not remove pre-existing data. The data must be overwritten using a software program specifically designed to overwrite existing data with a specific or randomly generated pattern of data. If run properly, it will make the data unrecoverable by computer forensics experts, although the computer forensics expert may be able to discover the date, time and specific program used to conduct the wiping. Methods for physical destruction of a hard drive include hitting with a strong physical force, such as dropping it from a great height or hitting it with an implement such as a hammer, setting it on fire so as to expose it to a heat in excess of 300 degrees Fahrenheit, by submerging the hard drive in water or shredding it. To effectively de-magnetise the hard drive a degaussing device (as opposed to ordinary magnet) must be used as this is the only device strong enough to disrupt the magnetic orientation of the data on the platters.

[3.3.4.3] Electronic data is durable and persistent and its persistence compounds at the rate which electronic documents accumulate. When faced with discovering documents for review in litigation, the owner of the documents may be faced with documents to review for relevance in the order of, potentially, millions.[315]

3.3.5 Dynamic, Changeable Content

[3.3.5.1] Electronic documents are dynamic and can be manipulated. Further, electronic documents, unlike hard copy documents, are rarely in a fixed final form.[316]

[3.3.5.2] The mere act of accessing or moving an electronic file may alter the data

[314] Australian Law Reform Commission, *The Hearsay Rule in Civil Proceedings*, Report 216 (1993) 3.
[315] Ibid.
[316] Ibid.

contained within it. Dynamic content in an electronic file may even be set to change over time without any human intervention. Examples of dynamic content include workflow systems that automatically update files and transfer data from one location to another, tape backup applications that move data from one cartridge to another, web pages that are constantly updated with information from other applications, and email systems that re-organise and remove data automatically.[317]

[3.3.5.3] It is this very fact that electronic documents are dynamic and changeable, that evidentiary procedures need to examine the computer system in which a document was created and ultimately stored, in order to be sure that the document has not been manipulated in undetectable ways.

3.3.6 Environment-Dependence and Obsolescence

[3.3.6.1] When removed from its environment, electronic data, unlike paper, may be unreadable. Without the proper software application needed to view the data, it would be incomprehensible. For example, data in a database will be meaningless if the data is removed from the database system in which it was created.

[3.3.6.2] Computers quickly become obsolete as technology changes and as users move towards different computer platforms. Personnel charged with retrieval of the information may not be familiar enough with an obsolete system to restore archived data for access. Accordingly, strategies to move archived data onto an up-to-date platform should be implemented and put into practice.[318] This is examined further in section 3.3.8.

3.3.7 Dispersion and Searchability

[3.3.7.1] Traditionally, hard copy documents were often organised in filing cabinets, with each project having its own file. By comparison, electronic documents typically remain disorganised in disparate locations. Although some organisations have document management systems which allow them to store all files in relation to a project together, many organisations do not have a structured system in which to organise electronic files; emails will be stored in email repositories and other files will be stored in a number of different locations, such as file servers, desktop computers, notebook computers, portable storage devices, removable media,

[317] Ibid.
[318] Australian Law Reform Commission, *The Hearsay Rule in Civil Proceedings*, above n 314.

backup tapes and even in the Cloud. Files could comprise emails and/or other electronic files including databases. Often the files will be replicated many times and there may be various versions of draft documents on the system.[319] Accordingly, it can be difficult to determine the provenance of an electronic document, as the ease with which electronic documents are created, edited and transmitted, may obscure the origins of a document.

[3.3.7.2] An advantage that electronic data has over hard copy is that it can be searched using automated tools,[320] and the tools for searching data are becoming more and more sophisticated. In addition to traditional keyword searching, concept searching is available, as is predictive coding, and these terms are explained further in section 5.4.

3.3.8 Accessible/Inaccessible

[3.3.8.1] Generally, information, whether it is hard copy or electronic information, may be inaccessible. In *Zubulake v UBS Warburg LLC* (*Zubulake 1*)[321] Shira Scheindlin J made this distinction between hard copy and electronic documents. Examples of inaccessible paper documents could include: (a) documents in storage in a difficult to reach place; (b) documents converted to microfiche and not easily readable; or (c) documents kept haphazardly, with no indexing system, in quantities that make page-by-page searches impracticable.[322] A further example not referred to by Scheindlin J, might be documents already lost or destroyed.

[3.3.8.2] Scheindlin J compared this to electronic data, where thanks to search engines, any data that is retained in a machine readable format is typically accessible. Whether electronic data is accessible or inaccessible turns largely on the media on which it is stored. Her Honour noted that there are five categories of data, listed in order from most accessible to least accessible, [323] which are (a) active, online data, examples of which include online hard drives;[324] (b) near-line data, examples of which include optical disks;[325] (c) offline

[319] Ibid 5.
[320] Ibid.
[321] 217 F.R.D. 309 (S.N.D.Y, 2003).
[322] Ibid 3.
[323] Ibid.
[324] n-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic record's life, when it is being created or received and processed, as well as when the access frequency is high and the required speed of access is very fast, i.e., milliseconds.
[325] This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records. Access speeds can range from as low as milliseconds if the media is already in a read device, up to 10-30 seconds for optical disk technology, and between 20-120 seconds for sequentially searched media, such as magnetic tape.

storage/archives, the principle difference between near-line data and offline data is that offline data lacks 'the coordinated control of an intelligent disk subsystem;'[326] (d) backup tapes, backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time consuming and expensive, especially given the lack of uniform standard governing data compression;[327] (e) erased, fragmented or damaged data, such data can only be accessed after significant processing.[328] Of these, the first three categories are typically identified as accessible, and the latter two as inaccessible. Information deemed 'accessible' is stored in a readily usable format. 'Inaccessible' data, on the other hand, is not readily usable. Backup tapes must be restored using a process similar to that previously described, fragmented data must be de-fragmented, and erased data must be reconstructed, all before the data is usable.

[3.3.8.3] In July 2009, the Sedona Conference's *Commentary on Inactive Information Sources*[329] further defined inactive data as 'orphaned', which is information within the organisation for which no one has knowledge or responsibility, 'legacy' information, which was created by or resides on systems or programs that the organisation no longer uses and 'dormant', which may technically have a custodian and may be in a format used by the organisation's current IT environment, but the information is not used or accessed. The Sedona Conference listed eight Inactive Information Guidance Principles:

> 1. Subject to any preservation obligations related to pending or reasonably anticipated litigation or government investigation, an organization should take reasonable steps to determine whether an inactive information store contains information that the organization should retain based on legal retention requirements or business needs.
> 2. Subject to any preservation obligations related to pending or reasonably anticipated litigation or government investigation, an organization should avoid excessive retention of

[326] This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered 'archival' in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near-line storage. Access speed may be minutes, hours, or even days, depending on the access effectiveness of the storage facility.

[327] A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to many gigabytes. Their transfer speeds also vary considerably. The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks. As a result, the data on a backup tape are not organized for retrieval of individual documents or files because the organization of the data mirrors the computer's structure, not the human records management structure.

[328] When a file is first created and saved, it is laid down on the storage media in contiguous clusters. As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and randomly placed throughout the disk. Such broken-up files are said to be 'fragmented'.

[329] The Sedona Conference, *Commentary on Inactive Information Sources*, (2009), <http://www.thesedonaconference.org> at 11 September 2015.

> inactive information by destroying it when it is no longer necessary to meet legal retention requirements or business needs.
> 3. An organization should take reasonable steps to determine whether an inactive information store contains information that is potentially relevant in a pending or reasonably anticipated litigation or government investigation.
> 4. An organization should take reasonable measures, through IT practices and user-facing policies and procedures, to reduce the ongoing accumulation of inactive information.
> 5. An organization should consider establishing policies and procedures for the orderly migration of data required to be retained or preserved to supported formats, systems and media to reduce the need to retain/preserve inactive information.
> 6. An organization should consider whether and how its policies/procedures regarding inactive information should apply to third parties in possession of the organization's inactive information.
> 7. An organization should consider periodically reviewing and updating any policies and procedures regarding inactive information to account for changes in laws, new forms of inactive information, and new technical capabilities or changes in business organization or requirements.
> 8. An organization should take reasonable steps to index/identify/organize/map corporate records (as reasonable, based on business needs) so as to minimize over-retention and disorganization.[330]

[3.3.8.4] Electronic information is so much easier to store than hard copy. One million documents can be stored on an external hard drive, which today, is less than the size a shoebox. While storage is cheap and easy, this means retrieving information for evidentiary purposes can be cumbersome and expensive, however, search tools are making retrieval much easier and targeted. These search tools are explored further in section 5.4.5.

3.4 Computer Networks and the Internet

[3.4.1.1] Computers are at the heart of electronic evidence; computers are used to create and store vast quantities of electronic evidence. Before the popularity of the personal computer, computers systems were generally stand-alone systems that consisted of a mainframe computer, connected to a number of devices to operate the computer. Today, computer networks like the Internet allow electronic evidence to be created by many users, shared and stored in various global locations.

[3.4.1.2] An understanding of the elements that comprise computer networks and the Internet is required, in order to understand how electronic evidence is created, exchanged and stored on such networks.

3.4.2 What is a Computer Network?

[3.4.2.1] A computer that is attached to one or more other computers, is known as a

[330] The Sedona Conference, *Commentary on Inactive Information Sources*, above n 329.

computer network and can include other devices such as printers, external hard drives, modems and routers. These are linked together and use software commands to exchange data.

[3.4.2.2] The simplest example of a network is a Local Area Network, for example, within an office. A Wide Area Network generally extends past one geographical location, for example, networking computers between offices located in Sydney and Melbourne, or even in London. An intranet is a private network of computers that generally uses the same protocols as the Internet to communicate between computers.

3.4.3 The Internet

[3.4.3.1] The Internet is a world-wide network of interconnected computers and networks that operates using a standard set of communication protocols called TCP/IP (transmission control protocol/Internet protocols). TCP/IP is so standardised, in fact, that it is built into all major computer operating systems.

[3.4.3.2] Each computer connected to the Internet, needs to have a unique address, and this is known as the computer's IP address. Until recently, IP addresses were in the form nnn.nnn.nnn.nnn, known as IPv4. However, this meant that only 2^{32} (4,294,967,296) IP addresses could be created. There is now a new Internet Protocol standard known as IPv6 which allows for 2^{128} IP addresses. These addresses are represented as eight groups of four hexadecimal digits separated by colons.

[3.4.3.3] If a computer connects to the Internet through an Internet Service Provider (ISP) then the ISP generally assigns a temporary IP address for the duration of the session. If the user connects to the Internet from a Local Area Network, the computer will have been assigned an IP address by the server, or a temporary one using DHCP (Dynamic Host Configuration Protocol). The difficulty of controlling who accesses the internet has been recognised by the High Court of Australia in *Dow Jones and Company Inc v Gutnick* (.[331]

[3.4.3.4] The way in which data is communicated via the Internet is the application in which the data is created transfers the data from what is known as the Application Layer (which is where the application to create the data is translated), to the Transmission Control Protocol (TCP) Layer. The data is passed along in 'packets' of data. The TCP layer passes that data to

[331] (2002) 210 CLR 575; 194 ALR 433 at [84].

the IP layer via a specific port number, and where each packet receives the IP address of the destination computer. The ISP's router examines the destination address in each packet so it knows where to send it. The data packets may pass through several routers before they end up at the destination computer. Once the packets arrive at the destination computer, they are translated back up the various layers to the Application Layer of the destination computer so the data can be translated for review by the recipient.[332]

[3.4.3.5] Domain names are IP addresses of computers which have been translated to a World Wide Web address that we can understand. For example. Domain Name Service providers keep a database of all domain names, so that the various domain names can be located. Therefore, when a user types in 'www.google.com' into a web browser, the home page displayed upon connecting to that site, is actually from the IP address of Google's server (which happens to be 74.125.237.198). Once the server is connected, Google's web server then displays information using Hypertext Transfer Protocol (HTTP). HTTP allows a web browser on a user's computer to send requests to web servers to download data from those web servers. A web server is computer that processes requests using HTTP, to distribute information on the World Wide Web. A web server can refer to the entire computer system, an appliance, or specifically to the software that accepts and supervises the HTTP requests.

3.5 Storage Media

[3.5.1.1] Electronic evidence is constituted by two main components, the storage device, and the content. The way in which data is stored is changing rapidly. First, there were mainframe computers which stored all data centrally, and users accessed the information via remote 'dumb' terminals. Next came the wave of personal computers where users were able to store data on their computers, as well as having centralised servers at the office.

[3.5.1.2] Today, cloud computing is becoming more popular. Instead of organisations having to purchase hardware upfront, bearing the burden of maintaining the hardware, replacing it every few years and employing staff to maintain it, organisations can now 'rent' server space from cloud providers. Refer to Section 3.5.8 for further detail on the Cloud.

[3.5.1.3] The contingent issues surrounding jurisdiction, security and privacy are still

[332] See further Narasimha Karumanchi, Dr A. Damodaram and Dr M. Sreenivasa Rao, 'Elements of Computer Networking: An Integrated Approach', 2014 CareerMonk Publications, pp 479-499

being worked through in this burgeoning area of e-commerce. However, it seems likely that cloud computing is accepted as a standard mode of data storage with the large benefits it brings to business, including cost savings. However, from an evidentiary perspective, cloud computing raises a whole new set of issues which are only starting to be identified.

3.5.2 The Personal Computer

[3.5.2.1] Much information that may be required for litigation purposes, may be stored on the hard drive of a personal computer.

[3.5.2.2] Personal computers are characterised by single-user systems based on microprocessors. The first personal computer arguably appeared in early 1975, and dubbed 'the Altair', although it did very little. Bill Gates and Paul Allen, began work on the BASIC programming language to use on the Altiar. However, it was Steve Wozniak, together with Steve Jobs, who created the first workable personal computer, which became known as the Apple Macintosh, and Wozniak and Jobs founded the Apple computer company together in 1976. Apple's personal computer was based on the premise that Apple would develop and own both the hardware and the software. Microsoft, founded by Gates and Allen in 1975, went on to develop DOS ('Disk Operating System') software to compete with Apple's operating system, which later became Windows. In 1981, IBM developed the 16-bit microprocessor which became known as the IBM PC, and IBM licenced 86-DOS from Microsoft, which became PC-DOS 1.0. This licence permitted Microsoft to sell DOS to other companies, which it did, and this product was known as MS-DOS. This meant that Microsoft could licence its operating system to any number of hardware vendors, and this gave Microsoft a leading market advantage during the 1980's and 1990's.[333]

[3.5.2.3] In the mid-1980s, the introduction of the 32-bit computer turned the PC into a valuable business tool. The 32-bit computer was capable of running multi-user programs at high speeds. The office desktop PC now contained enough computing power to run a small business. It is now common to link PCs together to form a network and the advent of the Internet means that users can access and download data that was created anywhere in the world. Other innovations included: the graphical user interface (GUI) so graphic symbols for

[333] See further Steve Wozniak with Gina Smith, 'iWoz: Computer Geek to Cult Icon: How I Invented the Personal Computer, Co-Founded Apple, and Had Fun Doing It', 2007 Steve Wozniak and Gina Smith.

computer functions could appear on the screen, and the Douglas Engelbart's 'X-Y Position Indicator for a Display System' which produced the 'mouse'.

[3.5.2.4] Both PCs and Apple Macintosh (Mac) computers allow data to be stored on storage media, such as an internal hard disk or an external device. This makes PCs and Macs a source of potential electronic evidence. Today, depending upon the way in which it is configured, the average personal computer can hold terabytes of data.

[3.5.2.5] An order may be obtained from a court to disclose certain contents of a hard drive of a PC, which may be delivered to a computer forensic expert for examination.

3.5.3 The Email Server

[3.5.3.1] The vast majority of business correspondence is now conducted via email, with or without an attachment. Emails are unique, in that 'emails deserve special attention at every level, retention, preservation, collection, production, and metadata – because of the evidentiary challenges presented. Emails present especially interesting evidentiary challenges because email systems are inherently insecure and unreliable.'[334]

[3.5.3.2] A recent decision of the Federal Court of Australia has confirmed that an email repository is a record keeping system,[335] and today is often the first place to start when looking for evidence during discovery. The reason is that almost all correspondence is delivered via email today, with attachments also comprising the correspondence. Email is highly relevant and can be narrowed down to dates and authors by utilising the metadata. Email is likely to contain the whole or at least part of an email thread, therefore, correspondence threads can be located easily in one place. However, it is recognised that a malicious third party may gain access to a senders' computer and initiate email correspondence, as emails are not 'signed' in the traditional way.

[3.5.3.3] Generally, most people either use a personal email account or a corporate account, even both. Various types of software exist to create, send, receive and store email.

---

[334] The Sedona Conference, *Commentary on Evidence & Admissibility*, (March 2008) <http://www.thesedonaconference.org> at 11 September 2015.

[335] *Australian Competition and Consumer Commission v Air New Zealand Limited (No 1)* (2012) 301 ALR 326 [57] (Perram J).

There are what's known as email client applications, and then there is webmail.[336] Software such as Microsoft Outlook and Mozilla Thunderbird are examples of email client applications, and require the user to download specific software onto their PC in order to access email. Webmail, however, allows a user to access email simply by logging onto the application via a standard web browser (standard web browsers include Microsoft Internet Explorer, Mozilla Firefox, Google Crome or Safari). The user does not need to download specific software.

[3.5.3.4] With corporate email, the email client will connect to the email server located on the corporation's servers, whether those servers are on the corporation's premises, or at a Cloud provider's premises. Either way, all email traffic is via the corporation's email server. Although generally, most corporations have their own privately owned, dedicated email server, some corporations can now take advantage of corporate email management plans, like that offered by Microsoft Office 365.[337] There, Microsoft can host a corporation's domain name, such as 'mycompany.com.au', and the corporation's administrator can create email accounts, to which email traffic is then directed. The client can either download the client application, Microsoft Outlook, to access their email, or login via Microsoft Office 365 site.[338]

[3.5.3.5] With webmail, all email traffic is directed through the webmail service provider to a specific individual. Examples of webmail services include Gmail, Hotmail, Outlook.com.

[3.5.3.6] Historically, POP (Post Office Protocol) accounts were once most common form of email, when email was first becoming popular. POP was created when bandwidth was very low.[339] Emails could therefore be downloaded from the server for offline review, and removed from the remote email server. The problem, however, was that the emails, once downloaded, were tied to a specific computer and could not be accessed on the server via webmail or any other means.

[3.5.3.7] IMAP (Internet Message Access Protocol), allows emails to be kept on the email server until the user deletes them. The issue, however, is that there is a limit on the mail box

[336] 'Email: What's the Difference Between POP3, IMAP, and Exchange?' *How-To-Geek*, <http://www.howtogeek.com/99423/email-whats-the-difference-in-pop3-imap-and-exchange/> at 5 January 2016.
[337] Microsoft Office 365 website: <https://products.office.com/en-US/> at 5 January 2016.
[338] Ibid.
[339] 'Email: What's the Difference Between POP3, IMAP, and Exchange?', above n 336.

size, so emails need to be deleted when the mailbox is full.

[3.5.3.8] Microsoft has developed its own email exchange protocol, known as MAPI (Messaging Application Programming Interface), specifically to allow emails to be communicated on Microsoft Exchange Servers and Microsoft products such as Microsoft Outlook.

3.5.4 The File Server

[3.5.4.1] A file server is essentially a computer that is attached to a network and is primarily used to provide a shared storage location for computer files. Personal computers attached to the network can access the files stored on the server.

[3.5.4.2] Evidence from a file server, can be obtained by a computer forensic expert, in the same way as for any other computer. If evidence is to be obtained from a Cloud provider, the user ID and password for access to the Cloud server will be required.

3.5.5 Backup Tapes

[3.5.5.1] 'Recovering evidential data from magnetic tapes in a forensically sound manner is a difficult task.'[340] To obtain a copy of a backup tape in a forensically sound manner, the examiner should not alter the original tape in any way.[341]

[3.5.5.2] Backup tapes are normally created for disaster recovery and business continuity purposes. Information that is stored on backup tapes and systems act as a reserve copy of the original to be accessed if anything happens to the original data. In the event of data loss, the backup tape can be accessed to restore the lost information.

[3.5.5.3] Given the volume of data that is created and often backed up on a daily basis, it is backup tapes that are often resorted to if discovery needs to be made of an organisation's electronic information and there is no other archival system available. The most likely reason for this is that, in litigation, an incident relevant to the issues, usually occurred at some point in the past, perhaps years ago, and the active data may no longer contain relevant files. Backup

[340] Bruce J Nikkel, 'Forensic acquisition and analysis of magnetic tapes' (2005) 2(1) *Digital Investigation* 8, 18.
[341] H. Marshall Jarrett and Michael W. Bailie, Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002) United States Department of Justice <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf > at 11 September 2015.

tape rotation systems and incremental backups ensure that weekly, monthly and annual backups are available for restoration and this also increases the complexity of a backup tape investigation. Conversely, the use of rotated tapes, whether they be full or incremental, can help a forensic investigator to create a time line of activity on files.

[3.5.5.4] Backup tapes are usually created using backup tape drives (hardware) and backup software. Most backup tape drives put compression algorithms in the hardware and so files are compressed at the tape block level. However, many backup software programs also contain compression methods. Usually, one compression method is used when information is backed up to tape. Decompression of hardware-related compression is generally done because the tape drive itself will perform the decompression. However, if the tape files were compressed using the backup software, it may be difficult to analyse the data without the original backup tape software or knowledge of the compression algorithm used. Some backup tape software allows for tape content to be encrypted as it is written to the tape and this increase the complexity of backup tape restoration.

[3.5.5.5] Backup tapes come in a large array of different formats and consequently the archive format of a backup tape file is not standard. There are some open formats common among Unix and Linux systems, but most operating systems and commercial backup providers use their own proprietary formats. The wide variety of formats can create issues when trying to recover the contents of a tape. Tapes are particularly vulnerable to damage and can be affected by humidity, dust, and smoke. Any attempts to copy or read from tapes should allow for handling of tapes to be minimised.

[3.5.5.6] One of the main reasons that restoration of backup tapes is expensive is that in the past, the same combination of tape drive (hardware) and software that was used to create the tape was required in order to restore the tape. Also, in order to access email, the whole environment from which the data was copied also had to be in place.

[3.5.5.7] For tapes that are years old, it will be unusual for the organisation to have kept legacy hardware or software, so restoration of tapes would require the tape drives to be obtained and if obsolete, to be rebuilt. Even if the equipment and the software could be obtained, the skills required to rebuild the environment may be hard to locate. Knowledge of the environment is often lost, since the IT personnel who created the tapes may no longer employed by the organisation. Even if the data can be restored, the archives will contain many duplicates

of the material and also many irrelevant files will be obtained through the process.

[3.5.5.8] The restoration of backup tapes should only be resorted to when relevant active data is unable to be located.

3.5.6 Removable Media & Portable Devices

[3.5.6.1] Removable media and portable devices are a form of storage media that sits outside the computer system. The files can be stored on any form of removable media, the size of which varies. Removable media and portable devices come in any number of formats, including Compact Disks (CDs), Digital Versatile Disks (DVDs), disks connected via Universal Serial Bus ('USB') and other devices such as those contained in cameras and mobile phones. These media are described further below.

[3.5.6.2] Disk formats include CD and DVD. CD-ROM is an acronym for Compact Disc Read Only Memory. This medium commonly store 650 megabytes, although some can store up to 1 gigabyte. CD-RW stands for Compact Disc-ReWritable, which means data can read and overwrite data on the CD. Compact Discs are not a long term storage medium as they can be corrupted easily.[342] DVD-ROMs can be read but not overwritten, DVD-R can record data once. DVD-RW can record and erase data. Discs can hold 4.7 gigabytes single sided or 8.5 gigabytes double sided. DVDs are also easily corrupted so they are not a long term storage medium.[343] Blu-ray, also known as Blu-ray Disc (BD) are designed to store large volumes of digital video. BD disks utilise a blue-violet laser to read and write data and hence, the name is a combination of 'Blue' (blue-violet laser) and 'Ray' (optical ray). These discs can hold 25 gigabytes on a single-layer disc and 50 gigabytes on a dual-layer disc (which equated to over 9 hours of high-definition (HD) video or about 23 hours of standard-definition (SD) video). Blu-ray discs are the next-generation optical disc format. The format was developed to enable recording, rewriting and playback of high-definition video (HD). BD-ROM is a read-only format for distribution of HD movies, games, software, etc., BD-R is the recordable format and BD-RW is the rewritable format.[344]

---

[342] See further: Teach-ICT.com: THE site for ICT education, <http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg7.htm> at 12 January 2015.
[343] See further: Teach-ICT.com: THE site for ICT education, <http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg8.htm> at 12 January 2015.
[344] See further: Teach-ICT.com: THE site for ICT education, <http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg9.htm> at 12 January 2015.

[3.5.6.3] Other types of external storage include those with Universal Serial Bus ('USB') connectivity to a computer. A flash memory data storage device integrated with a USB interface.[345] Storage capacity is ever-increasing. When a USB flash drive is plugged into a computer running a Windows operating system, a number of registry settings and log files are automatically updated to reflect the use of the USB flash drive and this can be particularly valuable in identifying what type of USB device was used, when it was accessed, what drive letter was assigned and so on.[346] A computer forensic expert can access the Windows registry to obtain such information. USB hard disk drives are available to store up to 1.5 terabytes, but this is ever increasing.

[3.5.6.4] CompactFlash (CF) is a mass storage device format used in portable electronic devices. CompactFlash typically uses flash memory for storage in a standardised enclosure. The physical format is now used for a variety of devices, such as digital cameras.[347]

[3.5.6.5] A digital video recorder (DVR) or personal video recorder (PVR) is a device that records video in a digital format to a disk drive or other medium such as handheld video recorders or via cameras and software.

[3.5.6.6] Digital mobile phones are capable of storing digital photos, digital video, digital audio (on voice mail stored with the provider) and of course text. The digital mobile phone can be a source of a great deal of potentially discoverable material. Each mobile phone will potentially use a SIM card (see below). Moreover, Mason posits that the range of electronic evidence associated with mobile phones extends to the mobile phones geographical location, not only the details of the calls made and received.[348]

[3.5.6.7] Subscriber Identity Module, or 'SIM Card', is a microchip which allows the mobile phone to function. The SIM card stores the phone's configuration data, and information about the phone itself, such as which calling plan the subscriber is using. A SIM Card can

---

[345] See further: Teach-ICT.com: THE site for ICT education, <http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg10.htm> at 12 January 2015.

[346] Paula Thomas and Alun Morris, 'An Investigation into the Development of an Anti-Forensic Tool to Obscure USB Flash Drive Device Information on a Windows XP Platform' (2008) *Third International Annual Workshop on Digital Forensics and Incident Analysis* 60-66; see also Nikkel, 'Forensic acquisition and analysis of magnetic tapes', above n 340, 12.

[347] See further: Techopedia <https://www.techopedia.com/definition/25275/compactflash-cf> at 12 January 2015.

[348] Mason, above n 178[1.28].

store some information, such as contacts. Each SIM Card is activated by use of a unique numerical identifier and once activated, the identifier is locked down and the card is permanently locked in to the activating network.[349]

[3.5.6.8] A digital audio player, often referred to as an MP3 player, is a consumer electronics device that stores, organises and plays audio files. Some digital audio players can also support image-viewing and/or video-playing support. MP3 players are now regularly built into mobile phones, making them the most common form of digital audio player.[350] Apple's iPod is becoming one of the most common digital audio players on the market. Mobile phones, MP3 and iPods all store files in the same way as other media and hence can be used to copy and store files in the same way as a USB flash drive or other portable media.

3.5.7 Storage in the 'Cloud'

[3.5.7.1] Cloud storage was referred to briefly in section [3.5.1.2]. The way cloud computing works is that a cloud provider can make any number of 'virtual' machines available on a single server and rent this space out to users. In this way, one server can be utilised by hundreds, even thousands of users, instead of one single user. Cost savings can be found for users in that they only pay for what they use and which means an organisation's information technology requirements can remain flexible.[351] Cloud users should be concerned that they can access their data at any time, and that it is kept secure.

[3.5.7.2] Generally speaking, cloud computing can be divided into three categories: (a) data storage: infrastructure as a service (IaaS); (b) application development: platform as a service (PaaS); and (c) software hosting: software as a service (SaaS).[352]

[3.5.7.3] Another feature of cloud computing is that cloud providers can load balance their data across many different servers, which might mean servers are located in different countries with different standards of protection, privacy and protocols. Cloud computing does raise a number of concerns which include data security and regulation, service level

[349] See further WiseGEEK: <http://www.wisegeek.com/what-is-a-sim-card.htm> at 12 January 2015.
[350] BBC WebWise: <http://www.bbc.co.uk/webwise/guides/about-mp3s> at 12 January 2015.
[351] See generally, Law Society of England & Wales, '*Cloud Computing*' Practice note, 7 April 2014, http://www.lawsociety.org.uk/support-services/advice/practice-notes/cloud-computing/, at 5 January 2016; New Zealand Law Society, '*Defining cloud computing*', <https://www.lawsociety.org.nz/lawtalk/lawtalk-archives/issue-845/defining-cloud-computing>, at 5 January 2016.
[352] National Institute of Standards and Technology website: <http://www.nist.gov/itl/cloud/index.cfm> at 11 September 2015.

requirements, availability of continuity of service, termination rights, ownership of data, privacy and jurisdictional issues. Some cloud contracts provide that the cloud vendor owns the data and if hosting fees are not paid, the user no longer has the right to access their data.[353] In court proceedings, this may be problematic as a litigant may first have to find out the jurisdiction in which the data is located, and then prove that they are entitled to have access to it. Depending upon the country in which the data is located, the government of that country may have regulatory conditions to enable access to the data.[354]

[3.5.7.4] With cloud computing, computer servers for one company can reside in more than one company and this, of course, can give rise to jurisdictional issues; not all jurisdictions have the same obligations with respect to privacy and data protection. Some examples illustrate these points. If data is stored in the United States of America, and many cloud providers do have servers in that country, then the data may be subject to the USA Patriot Act. The USA Patriot Act is an acronym for Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001, and its purpose is stated as to 'target terrorism' and is 'not intended to grant unfettered access to data'.[355] It applies to any organisation with a presence in the USA regardless of where data is held. Likewise, in the United States of America, pursuant to the *Stored Communications Act* (USA), a valid subpoena issued in relation to a criminal investigation can compel disclosure of basic subscriber records. A search warrant showing probable cause can compel disclosure of stored contents of any account including messages, photos, videos etc. Interestingly, Facebook[356] makes it clear in their 'data use policy' that information may be disclosed pursuant to a legal request including those outside of the USA. In Australia, the *Cybercrime Legislation Amendment Act 2012* (Cth) inserted provisions into the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access Act) 1979* (Cth) to preserve certain communication records.

[3.5.7.5] Jurisdictional issues are highlighted by a recent case where Microsoft was

[353] See, for example, *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281.

[354] Refer generally, National Archives of Australia, <http://www.naa.gov.au/Images/Check-up%202.0-All-Questions_tcm16-82787.pdf> at 11 September 2015.

[355] Parts of the USA Patriot Act expired on 1 June, 2015. The USA Freedom Act was passed 2 June, 2015 and the expired parts were restored and renewed through to 2019. However, section 215 was amended to stop the National Security Agency ('NSA') from continuing its mass phone data collection program, rather phone companies will retain the data and the NSA can obtain information about targeted individuals with permission from a federal court.

[356] Refer Facebook website: <http://www.facebook.com> at 11 September 2015.

ordered by a court in the United States of America to make available documents stored on servers in Ireland. In July 2014 in New York, US District Judge Loretta Preska, ruled that Microsoft must turn over a customer's emails which are stored in a data centre in Ireland to the US Government. Microsoft, along with other US companies, had challenged a criminal search warrant for the emails, saying that federal prosecutors cannot seize customer information that is held in foreign companies. However, the Judge ruled that the warrant lawfully required the company to hand over any data it controlled, regardless of where it was stored. 'It is a question of control, not a question of the location of that information,' Her Honour said.[357] In September, Microsoft's appeal to the Second U.S. Circuit Court of Appeals in Manhattan was argued, with a decision pending.[358] The 'Microsoft Ireland' case, as it has become known, is being keenly watched by global media, with a concern that a decision against Microsoft would create a 'global free-for-all'.[359]

[3.5.7.6] Schedule 1 of the *Privacy Act 1988* (Cth),[360] contains thirteen Australian Privacy Principles. Australian Privacy Principle 11 on Security of Personal Information states that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. Australian Privacy Principle 8 deals with trans-border data flows and states than an entity in Australia may only transfer personal information about an information to someone (other than the entity or the individual) who is in a foreign country only if the following set of criteria are satisfied:

> (a) the entity reasonably believes that:
> (i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
> (ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
> (b) both of the following apply:
> (i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;
> (ii) after being so informed, the individual consents to the disclosure; or
> (c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
> (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the

[357] *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, F. Supp. 2d., 2014 WL 1661004 (S.D.N.Y. 25 April 2014).
[358] *Microsoft Corporation v United States of America* ('Microsoft Ireland' case) Case number 14-2985-cv.
[359] The Washington Post, 'U.S. battle over Microsoft e-mails could result in "global free-for-all"', <https://www.washingtonpost.com/world/national-security/us-battle-over-microsoft-e-mails-could-result-in-global-free-for-all/2015/09/09/f8dcbf1e-5722-11e5-abe9-27d53f250b11_story.html>; as at 5 January 2016.
[360] *Privacy Act 1988* (Cth) Schedule 1.

table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

[3.5.7.7] In Australia, there has been much public discussion over the government's right to access metadata collected and stored by telecommunications carriers. The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) imposes data retention obligations on telecommunications carriers, carriage service providers and internet service providers. The *Telecommunications (Interception and Access) Act 1979* (Cth) already allows certain government bodies and agencies to gain access to telecommunications data (but not the content of the communications),[361] however, there was no obligation on carriers and carriage services providers to collect and store that data. The 2015 amendments provide for certain data to be retained for two years.[362] The data set has been specified in the Act and includes:

(a) Date and time of a communication (for example, the start/end time of a phone call, time an email or message is sent, or when a chat began);
(b) Type of communication (for example, SMS, phone call, email, video chat, social media platform) and
(c) Type of service used (for example, ADSL, cable, GPRS, Wi-Fi);
(d) Features of the service (for example, data volume usage, call forwarding, call waiting);
(e) Duration of a communication;
(f) Identifiers of the account (email addresses, phone numbers of incoming/outgoing caller, identification number of a mobile device used);
(g) Data on the status of the service and any related account or device; and
(h) Location of the equipment (phone, wifi hotspot, cell tower) at the beginning and end of the communication.[363]

[3.5.7.8] However, the data set does not include the content of emails or calls and does not include a user's web browsing history, log-in information or password. The data will be 'personal information' under the Privacy Act 1988 (Cth) and must be encrypted[364] (the type of encryption is not prescribed).

[361] *Telecommunications (Interception and Access) Act 1979* (Cth), Chapter 4.
[362] *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth), s 187C.
[363] Ibid s 187AA
[364] Ibid s 187BA.

[3.5.7.9] PricewaterhouseCoopers has estimated the cost to these services providers to retain this information to be between $188.1 million and $319.1 million,[365] although a service provider can apply for an exemption to encrypt data by offering 'alternative data retention or information security arrangements'.[366]

[3.5.7.10] In Europe, the European Union Data Protection Directive[367] (Directive 95/46/EC), sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of these data. Thus a company may be violating this EU directive if the data goes to services in prohibited countries but in many cases, the vendor cannot make contractual promises regarding the location of the data as they do not know where the data will be going. The Directive is currently under review.[368]

[3.5.7.11] There may be some complications concerning the preservation of documents when discovery ensues in a litigation case. Given that the data subject to discovery may actually reside in the cloud and not be readily accessible, and Australian courts would have no supervisory jurisdiction over the cloud provider, there are both issues with access and potential contamination of evidence. The outcome of the Microsoft Ireland case (refer section [3.5.8.5] above) may mean information can be obtained under search warrant; whether this extents to discovery of documents in civil litigation remains to be seen.

[3.5.7.12] To recover data stored in the Cloud, the data must be stored in Australia, the user must be entitled to access the data and the user needs to provide their login details in order to access the data. Without these elements, it may be difficult to obtain evidence that is stored in the Cloud.

---

[365] Commonwealth Attorney-General's Department's website: <http://www.ag.gov.au/dataretention> at 11 September 2015.

[366] *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth), s 187K.

[367] European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 24 October 1995.

[368] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation':
<https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf>, as at 5 January 2016.

3.6 Content

3.6.1 Email

[3.6.1.1] Email has by now, become the default standard means of correspondence.[369] Only a few years ago it was standard practice to correspond via hard copy, however, today almost all exchanges between people and organisations is via email with attachments. For the younger generation, the standard way to communicate is via social media.

[3.6.1.2] An email file, including any of its attachments, is evidence and should be retained and exchanged in its original, native format. Although the best evidence rule has been abolished, by the *Uniform Evidence Acts*[370] the original email in its 'native' form, should be tendered, by both the sender and the recipient (unless it is no longer available), because the native document will contain all of the evidence, including the metadata. A print out of the email will omit this crucial evidence. The email contains not only the human generated content, but also real evidence in the way of metadata such as Date Sent, To, From, as well as details of the servers from which the email originated and was received.

[3.6.1.3] Email can be stored in a number of different formats, depending upon the software that created the email. For evidentiary purposes, it is important to obtain the original, unmodified email message file including its attachments, as this is the only way an email can be proved. Some older email repositories stored email and attachments in a flat file structure which makes it difficult to retrieve and view emails and attachments without specialist assistance.'

[3.6.1.4] Indeed, email can be submitted as evidence for a number of purposes. The email may be offered to prove that the sender did communicate with another person or persons, in which the communication, and not the content, may be called into evidence. The email may be tendered to show the sender was at a particular location at a particular time, and this will be evidenced in the metadata showing the computer's IP address from which the email was sent.[371] If authenticity is still challenged, the actual sender of the email may have to give evidence of doing so. However, if the sender of the email denies having authored the email, then the party

[369] Monica E. Seeley, Gerard N. Hargreaves, Managing in the Email Office (Routledge, United Kingdom, 2003), 1.
[370] *Uniform Evidence Acts* s 51.
[371] *Greene v Associated Newspapers* [2005] QB 972,

tendering the email will need to provide a wide array of evidence in order to prove the identity of the sender. This may be difficult unless the party tendering the email has circumstantial evidence to show the sender was at a particular place at a particular time and on the balance of probabilities (for civil matters), did send the email.

3.6.2 Short Message Service ('SMS') and Instant Messaging ('IM')

[3.6.2.1] Short Messaging Services, or SMS, are text messages that are sent using a digital telephone, the World Wide Web or a mobile communications systems. SMS uses standard communication protocols in order to exchange short text messages.[372] Instant Messaging ('IM') offers real-time text transmission over the Internet, usually through a specific software application. Both SMS and IM are used as a less formal means of communication, and correspondence chains are stored and are capable of retrieval, just like any other form of electronic evidence.

[3.6.2.2] In the United States of America, the courts have said that there is no justification for constructing unique rules for admissibility of electronic communications such as instant messages and are to be evaluated on a case-by-case basis, as any other document, to determine whether or not there has been an adequate foundation showing of relevance and authenticity.[373]

[3.6.2.3] Instant Messaging via IM software or via Twitter can be particularly relevant for the purposes of electronic discovery if it is used to communicate between employees. Organisations should run IM over a corporate server so that traffic is kept and stored. Instructions about project deadlines, variables and changes to project plans are often relayed across applications such as IM, because it is faster than waiting for a response to an email. If the company ever needs to recall instructions received this way, it must be stored somewhere else where it is retrievable.

[3.6.2.4] The problem with instant communication applications is that people forget that they are creating a permanent record. They will often say things that they may not ordinarily say in an email, yet that information is just as easily discoverable. Conversely, because users often use shorthand due to time and space constraints, comments may be difficult to interpret

[372] Refer Techopedia: <https://www.techopedia.com/definition/24275/short-message-service--sms> at 12 January 2015.
[373] In the interest of *F.P., a Minor*, 2005 PA Super 220, 878 A.2d 91 (Pa.Super. 2005).

except by the sender. Ancillary evidence may be required to explain the content of IM or Twitter. To illustrate exactly how a simple message sent through instant communication applications can result in a legal complication, in July 2009, a lawsuit was filed in Chicago for allegedly defamatory remarks on Twitter by Amanda Bonnen, a tenant who posted a 140-character 'tweet' about her building's management company, Horizon Realty Group: 'You should just come anyway. Who said sleeping in a moldy apartment was bad for you? Horizon Realty think it's okay'.[374] The irony of the lawsuit, however, is that Ms Bonnen only had 20 followers at the time, yet the lawsuit has meant that the 'tweet' had been republished over and over in news stories and articles.

3.6.3 'Office' Electronic files

[3.6.3.1] While email tends to be stored in its own record keeping system electronic files such as correspondence generated in Microsoft Word, or spreadsheets, presentations, drawings and so on, are created and stored on their own. Each file is created using proprietary software and stored in a particular format which can only be interpreted by the proprietary software, although there are now tools available that can access the content of such files without the need to obtain the proprietary software, while recognising that it is in that proprietary format. Electronic files are often categorised as 'standard' and 'non-standard', with the 'standard' category being constantly updated as technology changes and proprietary formats change accordingly. Examples of 'standard' files include Microsoft Office files (Word, Excel, PowerPoint), Adobe Portable Document Format (PDF), Image files (such as TIFF, GIF, JPEG) and even CAD drawing files. If both parties to a litigation are using the same proprietary software and need to exchange files during discovery, those files may be categorised as 'standard' for the purposes of that litigation. If they are not using the same proprietary software, then one party may need to agree to provide a copy of that software to the other party, or otherwise agree as to how the software will be provided so that the evidence can be viewed.

3.6.4 Websites

[3.6.4.1] A website comprises related web pages that are generally served from a single web domain. The website can be hosted on one or more web servers (web servers hold and send information on the World Wide Web)[375] and is accessible via the Internet or a private

[374] *Horizon Group Management LLC v Bonnen*, Civ. No. 2009 L 8675 (Circ. Ct. Cook County, Ill. Jan. 27, 2010).
[375] *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 (28 August 2001) per Hedigan J at [14].

local area network. The Internet address of a website is known as a Uniform Resource Locator (URL) and all publicly accessible websites constitute the World Wide Web**.** Website pages are general dynamic and are being updated regularly by website domain owners. Website pages therefore, can alter frequently, so screen shot images are generally not reliable,[376] except if taken at a point in time of relevance to the issues in dispute.

3.6.5 Cookies

[3.6.5.1] A cookie is a small piece of data sent from a website and stored in a user's web browser while the user is accessing that website. Whenever a user goes back to that website, the browser sends the cookie back to web server so the server has information about the user's previous activity on the site.[377] A cookie can store information such as the user's browsing activities and information such as shopping cart items. Cookies can also be used to store log in details so that the web servers know whether the user is logged in or not. Cookie data can be encrypted to preserve security.

3.6.6 Social Media

[3.6.6.1] Information on social media sites has become a source of evidence in recent times, in both civil and criminal proceedings. The expression 'social media' encompasses a variety of platforms and includes social networking sites where users can create their own webpages and communicate with others via online chat, instant messaging services, blogging and even by voice or video. Examples of social networking sites include FaceBook,[378] MySpace, [379,] LinkedIn[380] and Reddit.[381] 'Tweeting' via the website Twitter[382] is another form of social media, where users upload short messages from their computers or smart phones; this can also be known as 'micro blogging'.[383]

[3.6.6.2] Blogging is becoming a form of publishing in its own right. Blogging is a form of social media where an author writes their own views on any particular subject, which is

[376] *R v Skinner* [2005] EWCA Crim 1439 (May LJ).
[377] *Amazon.com, Inc.* [2011] APO 28 (9 May 2011) at [28].
[378] Refer Facebook website: <http://www.facebook.com/> at 11 September 2015.
[379] Refer Myspace website: <http://www.myspace.com/> at 11 September 2015.
[380] Refer LinkedIn website: <http://www.linkedin.com/> at 11 September 2015.
[381] Refer Redit website: <http://www.reddit.com/> at 11 September 2015.
[382] Refer Twitter website: <http://www.twitter.com/> at 11 September 2015.
[383] See further Law Society of England & Wales, 'Social Media' Practice Note, 18 June 2015, <http://www.lawsociety.org.uk/support-services/advice/practice-notes/social-media/> at 5 January 2016.

published by the author on the Internet. Other users can then post comments on the site, giving feedback to the Blogger. Wikis are websites that allow users to add, remove or edit content, such as Wikipedia.[384] User generated sites allow users to create content, for example, YouTube[385] where users can upload videos and Flickr,[386] where users can share photos. RSS (Really Simple Syndication) refer to a web feed format used to publish content which is frequently updated such as blogs or podcasts; users can subscribe to their favourite feeds to be sure of receiving notification of updates. Mash-ups are websites that create content by combining content from different sources, such as iGoogle.

[3.6.6.3] To give an example of the explosion in the use of social networking sites, in May 2013, Facebook reached one billion users worldwide and has become the default method of communication for the current generation of teenagers. To demonstrate the ubiquitous nature of Facebook, in 2009, the Oxford Dictionary pronounced the word 'unfriend' (to remove someone as a friend on a social networking site such as Facebook) to be the word of the year. Social media has become another method of communication not only for teenagers, but for businesses as well, with many businesses now incorporating social media into their marketing initiatives to increase branding, through 'Twitter', podcasts, blogs, RSS feeds and so on. Indeed, in 2009, 'Twitter' was titled the 'top English word' based on a report from the Global Language Monitor which monitors the internet, media and electronic database to estimate how many times certain words or phrases are used.[387]

[3.6.6.4] Social media is now being used in commercial applications, with the result that the line between work and social activities is becoming blurred. PCWorld reports that a British study has found increased interactivity boosts surfing at work and careless chats while a related survey of more than 1,000 office workers has found that 42% of those aged between 18 and 29 discussed work-related issues on social networking sites and blogs,[388] while 59% of the same age group believed they should be entitled to access social media for personal use while at

[384] Refer Wikipedia website: <http://www.wikipedia.org/> at 11 September 2015.
[385] Refer Youtube website: <http://www.youtube.com/> at 11 September 2015.
[386] Refer Flickr website: <http://www.flickr.com/> at 11 September 2015.
[387] 'Twitter voted top English word', *The Telegraph* (online), 30 November 2009 <http://www.telegraph.co.uk/technology/twitter/6685906/Twitter-voted-top-English-word.html> at 11 September 2015.
[388] Tash Shifrin, *Is Web 2.0 a Security Risk?* (24 March 2007) PC World <http://www.pcworld.com/article/130114/is_web_20_a_security_risk.html> at 17 August 2015.

work using corporate computers.

[3.6.6.5] Social media is expanding the realm of electronic discovery and litigation, creating an information source that can, and has, become evidence, and is now part of the scope of discovery.[389]

[3.6.6.6] Another consideration is the infringement of copyright laws, which protect intellectual property in creative works. This aspect of legal protection is often ignored when information created by a third party is republished on social medial generated for personal use. When corporate information is made available on the Internet, users should be warned that using a third party's information on the Internet (or in any other way for that matter) could form a ground for infringement of copyright if permission is not obtained beforehand. In *Universal Music Australia Pty Ltd v Cooper*,[390] the Federal Court of Australia held that the proprietor of a website known as MP3s4free.com on which users could post hyperlinks to websites that provided infringing copies of music was liable for authorising infringement in relation to these links. Online service providers are obliged to remove material that infringes copyright where breaches are identified in section 116AH of the *Copyright Act 1968* (Cth).

[3.6.6.7] Privacy considerations also need to be taken into account. The Australian Privacy Principles[391] provide that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure and must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed.

3.6.7 Databases

[3.6.7.1] Information stored in databases is perhaps the best illustration of the differences between paper and electronic evidence. A database is a collection of data held in organised tables and columns, usually with a carefully thought out arrangement called a schema. Databases are accessed by database management systems (DBMSs) which are software

[389] Ethan J, Wall, 'Social Networking Sites Look Like Plunder to Attorneys', *Daily Business Review* (online) February 20 2009 <http://www.dailybusinessreview.com/id=1202428417060/Social-Networking-Sites-Look-Like-Plunder-to-Attorneys?slreturn=20140928212644> at 11 September 2015.
[390] (2005) 150 FCR 1.
[391] The Office of the Privacy Commissioner, *Australian Privacy Principles*, <http://www.privacy.gov.au> at September 2015.

applications that allow the user to interact with the database to capture and analyse data. Databases can be 'off-the-shelf' DMBSs such as Microsoft SQL Server, Oracle or dBASE, or they can be proprietary databases that have been custom built for a particular purpose. Databases are generally not portable across different DBMSs, however, databases can be generally be interoperable if they use standards such as SQL, ODBC or JDBC.

[3.6.7.2] Data stored in proprietary databases does need to be migrated from time to time for a number of reasons, including software no longer being supported, the need for hardware to be upgraded, technology modernisation programs intending to decommission legacy systems, and support staff to administer the software no longer being available.

[3.6.7.3] In migrating data from one platform to another, care must be taken so there are no changes or omissions to the data itself and this requires careful data mapping the data is transferred and stored in the same format as the original database. A stringent process must be used during the data migration process, and it must be possible reverse engineer the data migration. Data validation must be undertaken and steps taken to show that the evidential integrity has been maintained. These steps can be summarised as follows: (a) meaning – the meaning and the interpretation of the electronic data remains unchanged; (b) errors – any errors have been reasonably identified and satisfactorily explained; (c) transparency – the process is capable of being independently examined and verified; and (d) experience – the data migration is undertaken by personnel with proven experience in multiple data migration projects. A computer forensics expert would be best place to confirm these steps. See Section [5.2.1.4] for further explanation.

3.6.8 Log Files

[3.6.8.1] Logs are a primary source of identifying activity on a computer, since log files record transactional data, often chronologically. Log files can contain information about what activities have occurred over time, and so can be useful to piece together a chain of events, like a diary.

[3.6.8.2] Logs on computer systems include: system logs, audit logs, application logs, network management logs, network traffic capture, and data regarding the state of the file system. On networked computers, network traffic log files can assist in linking evidence across computers. Logs such as file access logs, process logs, network logs, application specific logs,

can be analysed, depending upon the nature of the case. Different systems provide different types of logging information and the quantity and detail of information on logs recorded can depend on the system and its default configuration. Often it is only system administrators who have access to log files, so a user would need to know how and where to access such files if they were to change them. Circumstantial evidence can be examined if log files have inconsistent dates or otherwise do not appear to be authentic.[392]

[3.6.8.3] Other information on the computer may be used to identify a given user. For example, other files on the computer can be viewed to see what was accessed by that user around the same time as the file in question. If, for example, a banking site was accessed that only the user could have accessed or other sites which required login access, these may all be used as corroborative evidence.

[3.6.8.4] Logs can be often used to provide circumstantial evidence. If a user's account can be shown to have been accessed at the time an incident occurred, the user may still claim that they 'didn't do it'.[393] If so, it may be necessary to supplement that circumstantial evidence with other evidence such as a physical (swipe card) logs and/or images from closed circuit television monitors to confirm the identity of the user, and the time of access to the system.

3.7 Electronic Evidence versus Paper Evidence

[3.7.1.1] The exposition above illustrates that there are so many different formats of electronic evidence, both media and content, highlights the fact that electronic evidence cannot be treated in the same way as paper evidence. The rules developed around documentary evidence clearly need to be reviewed. Computer technology means that vast stores of electronic evidence are created and stored every day. The Internet means that information can be exchanged with one another instantaneously and questions such as how to identify authors and how to authenticate evidence, which are at the foundation of the rules of evidence, are complex.

[3.7.1.2] The advent of the personal computer has allowed individuals to create and store electronic information. Organisations have been able to store larger and larger quantities of

[392] See further Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Elsevier, 3rd ed, 2011), 759-767.
[393] Ibid, 760.

information such that old methods of archival and records management are of no use. It is often necessary at the late stage of litigation to face an unstructured and often disorganised mass of data. Cloud computing has introduced global problems, because information can be stored in other international jurisdictions, and cloud contracts can provide that users do not, in fact, even own their data. This poses issues of security, privacy and confidentiality not address by existing legal rules.

[3.7.1.3] Authentication of electronic documents can lie in the metadata which is invisible when such documents are printed. Although not always relevant to the issues in a matter, the electronic version should always be kept intact, so that the document can be properly authenticated. If a hard copy only is available, a witness may be able to verify that they did, in fact, author the document. However, if the witness is not available, the document must be excluded as hearsay. Circumstantial evidence to prove that a witness did actually author a document is only possible if the metadata is available. It is necessary to examine how the courts deal with metadata and the fact it is an integral part of an electronic document.

[3.7.1.4] Databases, and compressed files that contain a number of other files, are examples of why paper and electronic documents are very different. There is no comparison in hard copy to a database or a compressed file, because each individual piece of paper can be viewed on its own and is not dependent upon a software application to pull out individual documents. This highlights the difficulty in using centuries' old rules in the authentication of electronic information.

[3.7.1.5] Consider the example of email, which is routinely admitted into evidence. Because email is hearsay, it needs to be tendered through a witness and if a business record, then as part of the Business Records Exception. Although email is now a common form of correspondence, it is unique because it does not bear a handwritten signature, as hard copy correspondence did in the past. Accordingly, to prove someone was the writer of an email, it is necessary to call the writer, or use circumstantial evidence. This is unique in the history of documentary evidence, where documents were often signed. Although it is not necessary that all documents be signed, other than those pursuant to the *Statute of Frauds*, a signature was often the best way to authenticate a document; that element of authentication is now removed with email, until a proven method of digital signatures has been developed and is accepted as a replacement for a handwritten signature. Given the cost and complexity of establishing a

public and private key through a gatekeeper, this may never occur. Proof of adoption of a 'document' is often critical evidence.

[3.7.1.6] Social media is another example of electronic evidence which is completely new and unique. Case law needs to be examined to see how the courts authenticate social media and whether current rules of evidence are being applied, or new rules of evidence are being created to properly authenticate such evidence.

[3.7.1.7] The next Chapter reviews the rules of evidence as they have been applied in Australia. There has not been a comprehensive review undertaken of the types of electronic evidence and how the reception of electronic evidence in a variety of forms should be treated by the law.

3.8 Summary & Conclusion

[3.8.1.1] Following an analysis of the nature of electronic evidence, it is clear that it is very different to paper. This leads to the next Chapter, which analyses the existing rules of evidence as they apply to electronic evidence. In particular, the definition of 'document' in the *Uniform Evidence Acts* and how this definition compares with definitions in other jurisdictions. The next Chapter also examines how courts recognise the various components that comprise electronic evidence and look at the Business Records Exception to the rule against hearsay. Finally, the next Chapter summarises a large part of the litigation process, discovery (or disclosure), since this is often where evidence is collected and reviewed.

4. CHAPTER 4 ANALYSIS OF EXISTING RULES OF EVIDENCE VIS-A-VIS ELECTRONIC EVIDENCE

4.1 Introduction

[4.1.1.1] In Chapter 2, an analysis of the laws of evidence around paper documents was undertaken, and it was demonstrated that the current rules of documentary evidence were developed over centuries. Those rules early rigidity in application gave rise to a number of exceptions that were developed due to exigencies of commerce. Chapter 3 analysed the various types of electronic evidence, and in this Chapter 4, how documents are defined in legislature and applied by the courts will be examined, as will the Business Records Exception.

4.2 Definition of a 'document'

[4.2.1.1] The Oxford dictionary defines a document as 'a piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record'. However, what does the statutory definition of 'document' comprise? In a number of jurisdictions, legislation has been enacted to provide a definition of 'document'. In Australia, the *Uniform Evidence Acts* define a 'document'[394] as 'any record of information'[395] and includes 'anything on which there is writing',[396] 'anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them',[397] 'anything from which sounds, images or writings can be reproduced with or without the aid of anything else'[398] or 'a map, plan, drawing or photograph',[399] and this definition is broad enough to include electronic records and documents. Other Australian jurisdictions have similar definitions which are also broad enough to cover electronic records and documents. The

[394] *Evidence Act 1995* (Cth) s 3 (definition of 'document'), *Evidence Act 1995* (NSW) s 3 (definition of 'document'), *Evidence Act 2008* (Vic) s 3 (definition of 'document') and *Evidence Act 2001* (Tas) s 3 (definition of 'document').

[395] A 'record' is defined in the *Acts Interpretation Act 1901* (Cth) to include information stored or recorded by means of a computer.

[396] *Evidence Act 1995* (Cth) s 3 (definition of 'document' (a)), *Evidence Act 1995* (NSW) s 3 (definition of 'document' (a)), *Evidence Act 2008* (Vic) s 3 (definition of 'document' (a)) and *Evidence Act 2001* (Tas) s 3 (definition of 'document' (a)).

[397] *Evidence Act 1995* (Cth) s 3 (definition of 'document' (b)), *Evidence Act 1995* (NSW) s 3 (definition of 'document' (b)), *Evidence Act 2008* (Vic) s 3 (definition of 'document' (b)) and *Evidence Act 2001* (Tas) s 3 (definition of 'document' (b)).

[398] *Evidence Act 1995 (Cth)* s 3 (definition of 'document' (c)), *Evidence Act 1995* (NSW) s 3 (definition of 'document' (c)), *Evidence Act 2008* (Vic) s 3 (definition of 'document' (c)) and *Evidence Act 2001* (Tas) s 3 (definition of 'document' (c)).

[399] *Evidence Act 1995 (Cth)* s 3 (definition of 'document' (d)), *Evidence Act 1995* (NSW) s 3 (definition of 'document' (d)), *Evidence Act 2008* (Vic) s 3 (definition of 'document' (d)) and *Evidence Act 2001* (Tas) s 3 (definition of 'document' (d)).

various definitions in each Australian jurisdiction are set out in Appendix A.[400] The expression 'writing' is also defined in most *Acts Interpretation Acts* to include electronic representation.

[4.2.1.2] Other jurisdictions too have variously attempted to define 'document', and these are summarised in Appendix B. The various definitions are broad enough to cover electronic records and documents and in England & Wales, the definition contained in the *Civil Procedure Rules* 2005 (Eng) provides that a 'document' includes anything in which information of any description is recorded,[401] and includes a definition of an 'electronic document' which specifies email and other electronic communications such as text messages and voicemail, word-processed documents and databases and documents stored on portable devices as well as documents that are readily accessible from computer systems and other electronic devices and media, including documents stored on servers, backup-up systems and documents that have been deleted. It also includes metadata and other embedded data which is not visible on screen or on a print out.[402]

[4.2.1.3] The definition of 'document' contained in the United States of America's *Federal Rules of Civil Procedure* (USA) include electronically stored information[403] and in Canada, the *Canada Evidence Act*[404] includes a definition of 'electronic document',[405] defined as 'data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print out or other output of that data'. The *Canada Evidence Act* also includes a definition of an 'electronic documents system'[406] as 'a computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic documents'.

[4.2.1.4] An analysis of court decisions that have applied the definition of 'document' is has been undertaken. Where no specific definition of 'electronic document' is provided in

[400] The expression 'writing' has also been defined to include electronic representations: *Acts Interpretation Act 1901* (Cth) s 2B.
[401] In England & Wales, the *Data Protection Act 1998* (Eng), Part 1(a) to (c) make it clear that information that is recorded on a computer, or is intended to be held on a computer, is data. Data is also information recorded on paper if it is intended that it is to be put onto a computer.
[402] *Civil Procedure Rules 2005* (Eng) r. 31.4.
[403] *Federal Rules of Civil Procedure* (USA) Fed. R. Civ. P, § r 34(a)(1)(A) (Cornell University Law School, 2010).
[404] *Canada Evidence Act* (R.S.C., 1985, c. C-5).
[405] Ibid s 31.8.
[406] Ibid.

legislation, the courts apply the generic definition to an electronic document and this also requires analysis. The analysis reveals inconsistencies and contradictions.

4.3 How the Courts Define 'Document'

[4.3.1.1] Although a 'document' does not need to be on paper,[407] the definition of 'document' in the *Uniform Evidence Acts* confirms that a 'document' does includes anything in electronic format.[408] What is meant by this expression, and how has this definition been applied by the courts?

[4.3.1.2] In Chapter 3, the various types of media upon which electronic documents are stored were identified and these include hard drives, backup tapes and portable media such as CD-Roms and DVDs. Further, the various document formats were discussed in which content is created, such as databases, word processing applications and email. However, do the courts distinguish between storage media and content? The short answer appears to be that they do not. Is this distinction meaningful and if so, why? Courts understanding of the way in which computer systems appears including how electronic information is created and stored, appears to be limited; rather, the courts tend to assume that electronic documents are basically the same as paper documents.

4.3.2 Storage Media - General

[4.3.2.1] Media such as hard drives do contain a wide variety of information, some of which could be privileged or not relevant to the issues in the matter. However, the way in which courts deal with this situation, and the guidance provided on how to deal with such information, is inconsistent, as demonstrated by the cases below.

[4.3.2.2] It is appropriate to consider the position in Australian and then compare treatment of the same issue in other common law jurisdictions.

---

[407] *R v Daye* [1908] 2 KB 333.

[408] In *Kennedy v Information Commissioner and another* [2010] EWHC 475, the court considered the word 'document' in the *Freedom of Information Act 2000* (Eng) s 32(2), and whether it encompassed electronic documents as well as hard copy documents. The court ultimately held that the word 'documents' was not confined to hard copy documents, including electronic documents.

4.3.3 Storage Media - Australia

[4.3.3.1] In Australia, computer records have been held to be admissible as documents.[409] Further, media such as CD-Roms, backup tapes[410] and hard drives have been held by the Federal Court of Australia in *Sony Music Entertainment (Australia) Ltd & Ors v University of Tasmania & Ors*[411] to fall within the definition of 'document' pursuant to the *Evidence Act 1995* (Cth). This was despite an argument that significant quantities of irrelevant documents would be produced. In that case, the respondents argued that the term 'document' should be applied to the records stored on electronic backup tapes,[412] CD-Roms and hard drives[413] and that each item of information on the hard drive, CD-Rom or backup tape should be considered a part of an electronic record and therefore discrete documents. This would have allowed each document to be considered individually to determine whether it was relevant and, therefore, discoverable. Tamberlin J, confirmed that the expression 'document' as used in the *Federal Court Rules* is defined[414] as per the definition in the *Evidence Act 1995* (Cth). His Honour referred to *Derby & Co Ltd v Weldon and others (No 9)*[415] where Vinelott J held that when referring to discovery of electronic information 'the party seeking discovery cannot be allowed simply to seat himself at his opponent's computer console and be provided with all necessary access keys',[416] as confidential and privileged documents need to be protected.

[4.3.3.2] Tamberlin J considered the evidence of a computer forensic expert retained by the applicant who gave evidence as to search terms to be used to identify relevant material. Further, Tamberlin J found that the scope of the *Federal Court Rules*[417] conferred a wide discretion upon the court and in this instance the definition of 'document' ought to be given

---

[409] In *TLC Consulting Services Pty Ltd v Paul Michael White* [2003] QCA 131 (21 March 2003). De Jersey CJ held, with Davies and Atkinson JJA agreeing, that a computer was a record for the purposes of *Fair Trading Act 1989* (Qld) s 89(1)(e)(i), and computer records were admissible as 'documents'. A preservation order was made ensuring a mirror copy of the computer's hard drive was created and deposited with the court.

[410] The English Courts have ordered the restoration of backup tapes in order to retrieve and search email accounts, notwithstanding the burden of doing so: *Digicel v Cable & Wireless* [2009] 2 All ER 1094.

[411] (2003) 198 ALR 367.

[412] Parties have been ordered to restore backup tapes to recover deleted emails and their attachments, despite the fact that such a task was burdensome. See *BT (Australasia) Pty Ltd v State of New South Wales & Anor (No 9)* [1998] FCA 363 where the court held that a party obliged to discover documents is obliged to discover data or information stored or recorded by electronic means.

[413] Similarly, discovery has been ordered of all computer tapes containing and/or recording any or all of the material required to enable a party to identify prospective defendants: *London Economics (Aust) Pty Ltd v Frontier Economics Pty Ltd* [1999] FCA 932 (30 June 1999).

[414] Australia, Federal Court of Australia, *Federal Court Rules* O 1 r 4.

[415] [1991] 1 WLR 652.

[416] *Sony Music Entertainment (Australia) Ltd & Ors v University of Tasmania & Ors* (2003) 198 ALR 367, 60.

[417] Australia, Federal Court of Australia, *Federal Court Rules* O 15A.

the fullest possible scope. His Honour stated that he was satisfied that 'as a question of jurisdiction the Court has power to order discovery of a CD-ROM, tapes or the other electronic storage devices which come within the definition of a document notwithstanding that they include a wide range of other information'.[418] The court found that it was appropriate to give discovery on the basis that an undertaking as to strict non-disclosure and confidentiality by the applicant's computer forensic expert, access be given to search across the material.[419] The court approved a process whereby a copy of the material was to be given to the applicant's computer forensic expert[420] and the respondents were to have the opportunity to see if they have any claims for privilege or confidentiality.[421]

[4.3.3.3] With the greatest of respect, while Tamberlin J made the correct decision to allow discovery of the hard drives, CD-Roms and backup tapes on the undertaking that strict non-disclosure and confidentiality be preserved by the applicant's computer forensic expert, the decision gives little guidance on the nature of electronic documents, which reside on electronic media as items of evidence. The decision allowed the computer forensics expert to undertake specific searches of a large body of electronic information in order to locate potentially relevant material. The discovering party was then afforded the opportunity to identify any privileged or confidential information and it is at this point that documents had to be identified specifically. However, the court did not provide useful analysis as to the nature of electronic documents and that fact that electronic media is merely a repository, much like a filing cabinet full of paper documents.

[4.3.3.4] Subsequent cases have not provided any further illumination. In *Jacques Nominees Pty Ltd v National Mutual Trustees Pty Ltd*[422] the Tribunal refused to overturn orders for a hard drive to be discoverable while recognising that it would be likely to contain a large volume of irrelevant and privileged material, and asked the parties to submit proposals on how to screen or mask such material.

[4.3.3.5] The problem posed by forensic images was highlighted in *GT Corporation v Amare*.[423] Forensic images are exact bit-for-bit copies of computer hard drives. In that case,

[418] Ibid 54.
[419] Ibid 68.
[420] Ibid.
[421] Ibid.
[422] (2000) V ConvR, 58-547.
[423] [2007] VSC 123 (25 May 2007).

the court considered the scope of forensic images as discoverable documents and highlighted the fact that one electronic repository can contain any number of documents. Amare had produced several forensic images for discovery. A forensic image is created when a forensic expert takes a bit-for-bit copy of the hard drive of a computer, meaning that the forensic images can contain many thousands, even millions, of files. By listing a forensic image as a 'document', Amare was in fact listing a very large bundle of documents without reviewing each single document. As a result, Amare later realised it had inadvertently produced a number of privileged documents on the forensic image. The court ordered Amare to swear an affidavit which listed 'each and every document, including each attachment, contained in its electronic discovery in respect of which it wishes to claim privilege'. Although not analysed explicitly, this case could be interpreted as suggesting that court-ordered discovery of a hard drive is in itself beset with privilege issues should a hard drive be viewed as a document. This decision raises interesting issues of process in disclosure of hard drives.

[4.3.3.6] The imaging of hard drives is a widespread phenomenon in modern insolvency and litigation practice.[424] Such images are frequently before the court as are the experts involved in their production',[425] and if a solicitor lacks the technical skills to access a computer hard drive, then appropriately qualified experts are available. Likewise, in the United States of America, forensic imaging and the use of computer forensic experts is widely permitted to allow one party to locate particular documents.[426] The court has also ordered authentication of images via comparison of the MD5 hash algorithm values[427] to the originals.[428] Further, the court has held that as long as chain of custody procedures have been maintained, the court will allow forensic images to be used.[429] The restoration of backup tapes may be ordered unless the court can be satisfied on the evidence that the material likely to be found is likely to be insubstantial, notwithstanding that the requirement to do so would impose a substantial burden

[424] *Porter v Australian Prudential Regulation Authority* (2010) 265 ALR 322.
[425] Ibid 46.
[426] *Re Honza* 242 S.W.3d 578, 583 n.8 (Tex. App. Waco 2008) the court said that a party may obtain discovery of 'the existence, description, nature, custody, condition, location and contents of documents and tangible things (including papers, books, accounts, drawings, graphs, charts, photographs, electronic or videotape recordings, data and data compilations) that constitute or contain matters relevant to the subject matter of the action'.
[427] Refer section [3.3.3.3] for an explanation of MD5 hash algorithm values.
[428] *Xpel Tech. Corp. v. Am. Filter Film Distributors* 2008 WL 744837 (W.D.Tex. Mar. 17, 2008).
[429] *Trammell v Anderson Coll* 2006 WL 1997425 (D.S.C. July 17, 2006) where an image of a hard drive had been made and emails were to be authenticated. The court accepted that there had been no alterations made from the time the image was made to the time of the hearing.

upon the respondent party.[430] Similarly, it has been held that a party must review backup tapes for the purposes of ascertaining whether they contain relevant material at all.[431]

4.3.4 Storage Media – England & Wales

[4.3.4.1] In England & Wales, earlier decisions appeared to confirm that certain electronic devices could be a 'document', [432] but also appeared to confuse the meaning of documents and information.[433] In *Victor Chandler International Ltd v Customs and Excise Commissioners and another*[434] the court held that 'information of itself cannot constitute a document, and the transmission of information of itself cannot constitute the transmission of a document'.[435] However, with the greatest of respect to Lightman J, if information of itself cannot constitute a document, then what is information?

[4.3.4.2] In 2005, in England & Wales, the definition of 'electronic document' was introduced into the Practice Direction 31B as a supplement to *Civil Procedure Rules* 2005 (Eng) part 31. Despite this practice direction, the courts are still allowing hard drives, and other devices, to be defined as a 'document', in particular, stating that a 'computer disc comes within the meaning of 'document' in *Civil Procedure Rules* 2005 (Eng), part 31.4.[436] Similarly, it has been held that a hard disk is not simply a container of files but is a single object containing a variety of materials,[437] and that a hard disk is a single storage entity which falls within the

---

[430] *NT Power Generation Pty Ltd v Power and Water Authority* [1999] FCA 1623 (9 November 1999).

[431] *BT (Australasia) Pty Ltd v State of New South Wales & Anor (No 9)* [1998] FCA 363 (Sackville J).

[432] In *Rollo v Her Majesty's Advocate* 1997 SLT 958 where a memomaster was held to be a legal 'document'. There, the police took possession of a memomaster and used it substantially in the trial of the accused for contraventions of the *Misuse of Drugs Act 1971* (Eng). The accused appealed on the basis that the contents of the memomaster were not evidence because it was not a 'document' as per *Misuse of Drugs Act 1971* (Eng) s 23(3)(b). The court held that although the word 'document' in normal usage does not refer to the means of storage or surface for storage, that does not mean legally such items cannot qualify as 'documents'. The court emphasised that 'the essential essence of a document is that it is something containing recorded information of some sort' and the fact that it is protected against unwanted access does not disqualify the memomaster from being a 'document'.

[433] In *Victor Chandler International Ltd v Customs and Excise Commissioners and another* [2000] 1 All ER 160 the court qualified that information itself cannot constitute a document, however, with respect, this seems contrary to the intention that all forms of electronic information be included within the definition of 'document'. In that case, the court was faced with the question of whether Teletext broadcast or Teletext pages, as they appeared on the screens of viewers, were 'documents'? The court held that the Teletext pages were found to be merely transmitted information and the screens on which they are seen are merely equipment for this transmission. Lightman J held that 'a document is a material object which contains information capable of extraction from it (e.g. a tape so long as it is not blank).

[434] [2000] 1 All ER 160.

[435] Ibid [11].

[436] *Phaestos Ltd v Ho* [2012] EWHC 2756 (QB).

[437] *R v Commissioners of Her Majesty's Revenue and Customs* [2011] 1 WLR 1964. However, interestingly, Forbes J rejected a submission that a warrant did not extend to a computer because 'the data stored electronically

definition of a 'document'.[438] The question remains whether this definition is too broad, or whether the courts still lack understanding as to the true nature of electronic information. It is suggested, with the greatest of respect, that the definition does remain far too broad, and an analysis of how the definition can be narrowed, without limiting the discretion of the court to accept relevant evidence, needs to be further examined.

4.3.5 Storage Media – United States of America

[4.3.5.1] In the United States of America, courts have differed in their opinions as to whether a hard drive constitutes a discoverable document, although the courts generally require that the party making the application do show some grounds for requesting discovery, and not go on a 'fishing expedition'.[439] Rather, the requesting party must demonstrate the particular elements of the electronic storage devices involved, the familiarity of its experts with those characteristics, or a reasonable likelihood that the proposed search methodology would produce the information sought.[440]

[4.3.5.2] A protocol that can be adopted in the United States of America is that the party seeking discovery selects a forensic expert to make a mirror image of the computer hard drive and perform the analysis with a protective order prohibiting disclosure of privileged information. The expert then provides a report of the documents or copies of the documents to the party opposing discovery who can review the documents and separate the privileged

on either the hard disk of the base units of the computer in question or on the floppy disks were all documents for the purposes of the warrant'.

[438] *R v Thames Magistrates Court, ex parte Da Costa & Co* [2002] EWHC 40 (Admin).

[439] In *Playboy Enterprises Inc v Welles* 78 F. Supp. 2d 1066 (S.D. Cal. 1998), the court ordered a mirror image be taken of the hard drive while in *Fennell v First Step Designs Ltd* 83 F.3d 526, 532-33 (1st Cir. 1996), the protocol submitted by Fennell was held to be inadequate, making discovery too much of a 'fishing expedition'. In *Re: Ford Motor Company* 345 F.3d 1315, 1316 (11th Cir. 2003), it was held that direct access to a database requires a factual finding of non-compliance with previous discovery rules/orders. However, in *Jones v Goord*, 95 Civ. 8026 (GEL) (S.D.N.Y. May 15, 2002) a request for discovery of state databases was denied on the basis of relevance, privilege, security, burden and costs.

[440] *Re: Weekley Homes* LP 180 S.W 3d 127 (Tex. 2005), which was an appeal from a decision where the courts had ordered experts to make forensic images of hard drives and then use a list of 20 key terms to search the forensic images for the documents requested, and then provide copies of the responsive documents to Weekley's lawyers to designate irrelevance, non-discovery or privileged documents. Weekley argued that the relevant rules do not identify access to computer drives as permissible discovery and that the rules did not permit the hard drive to be removed from the owner and searched by the other side. The court held that that the trial court abused its discretion in ordering the turnover of the employee computers for forensic examination on the basis that the plaintiff failed to demonstrate the particular elements of the electronic storage devices involved, the familiarity of its experts with those characteristics, or a reasonable likelihood that the proposed search methodology would produce the information sought.

documents. This protocol was manifested in *Sony BMG Music Entertainment v Arellanes,*[441] where the court refused Sony unfettered access to the hard drive but rather access through an appointed computer forensics expert. Similarly, in *Covad Communs Co v Revonet Inc,*[442] the court ordered a forensic image of the defendant's database data. In this case, the plaintiffs argued that they not only needed access to the defendant's database used for outbound and inbound leads but also to the electronically stored information outside of the relevant marketing campaigns. Accordingly, the plaintiffs submitted that they needed a forensic image to search the defendant's historical database but the defendant argued that the database had 'confidential' material and that imaging was not appropriate. The court ultimately sided with the plaintiff stating that any confidentiality or privilege issues could be addressed with a protective order. This appears to be sensible in that the court took into account the fact that the forensic image contained many items of potential evidence, and could not be considered on its own.

4.3.6 Storage Media - Canada

[4.3.6.1] In Canada, earlier cases did consider various forms of electronic media to comprise a 'document.[443] However, more recently, the courts have taken into account that fact that a hard drive is not a 'document' of itself, but rather, contains many different types of documents and can include privileged, confidential, irrelevant and even private information. The Canadian courts will consider whether a request to access a hard drive will require evidence that demonstrates a real likelihood that documents not disclosed exist or have existed, based on more than a mere suspicion.[444]

[4.3.6.2] The Canadian courts have had cause to examine the concept of a hard drive as a discoverable document on a number of occasions. Courts have denied production of the whole hard drive, and instead ordered that the requesting party was only entitled to production of the

[441] 2006 U.S. Dist. LEXIS 78399 (E.D. Tex. Oct. 27, 2006).
[442] 2009 U.S. Dist. LEXIS 47841(D.D.C. May 27, 2009).
[443] In *Reichmann v Toronto Life Publishing Company* (1990) 66 DLR (4th) 162 (Ontario Court of Justice) the court held that the diskette was included in the definition of 'document' in the Rules and that the computer disks on which manuscripts were stored were documents. In *Cholakis v Cholakis* 2000 CanLII 20735 (MB QB), a computer disk containing accounting data was held to be a discoverable document.
[444] *Nicolardi v Daley* [2002] OJ No. 595 (ON.S.C.) (QL). *Baldwin Janzen Insurance Services (2004) Ltd v Janzen* [2006] BCJ No. 753 (BCSC) (QL) demonstrated this point; in that case, the Court held that the production of a mirror image of a hard drive would not be ordered in the absence of evidence that the relevant documents had been withheld. See also *Desgagne v Yuen et all* 2006 BCSC 955 where an application to have a Palm Pilot delivered to an expert for review was denied on the basis it was not relevant.

relevant electronic data residing on the hard drive, and not the hard drive itself,[445] thereby recognising the distinction between the content and the storage media. The British Columbia Supreme Court has held that while courts do have the authority to order the production of electronic devices on which information is stored, an order to produce hard drives and personal computers may be refused due to relevance.[446] The Canadian courts may allow access to a hard drive to recover data where proper evidence has been produced illustrating that evidence may have been deleted from a computer. In such circumstances, the court may allow an expert to access the hard drive in an attempt to recover the deleted data,[447] although the court may refuse due to privacy and cost issues, where the probative value is outweighed by these considerations.[448]

[4.3.6.3] In Canada, the Supreme Court of British Columbia has held that only in exceptional circumstances will there be an order for production of a hard drive for examination by an expert, for example, where a party is intentionally deleting evidence or thwarting discovery. In *Innovative Health Group Inc. v Calgary Health Region ,*[449] Innovative Health Group appealed against an order to produce copies of its business hard drives being held in court (imaged hard drives). The issue in question was whether the case management judge erred in ordering production of the imaged hard drives. In her judgment, Madam Justice Conrad said:

> The case management judge erred in ordering production of the imaged hard drives. Although relevant and material information stored on a computer hard drive is producible, a hard drive is not ordinarily subject to production. In exceptional circumstances, a court can order production of a hard drive for examination by an expert, on appropriate terms, but only where evidence establishes that a party is intentionally deleting relevant and material information or otherwise deliberately thwarting the discovery process. Even in such a case, the applying party is only entitled to relevant and material information and it is the duty of the judge to protect irrelevant, confidential and private material. In this case, exceptional circumstances did not exist.[450]

[4.3.6.4] Innovative Health Group had argued that a computer hard drive was an

---

[445] *Mettech Corp v Metcon Service Ltd* [1996] BCJ No 1915 (BCSC) (QL).
[446] *Value Analytix Ltd v Doman Industries Ltd* [2002] OJ No. 595 (ON.S.C.) (QL).
[447] *Nicolardi v Daley* [2002] OJ No. 595 (ON.S.C.) (QL).
[448] *Ireland v Low* [2006] BCJ No 1592 (BCSC) (QL). In that case, the British Columbia Supreme Court refused to grant the defendant an order permitting a computer expert to forensically examine the plaintiff's hard drive and make copies of all files, including deleted files. Though the documents may have been relevant, their probative value was outweighed by considerations such as privacy interests, the availability of the evidence elsewhere, and the cost. Compare *Chadwick v Canada* [2008] BCSC 851 where the court ordered production of a hard drive for analysis by a computer forensic expert (even without exceptional circumstances).
[449] 2008 ABCA 219 (CanLII)
[450] Ibid [3].

electronic filing cabinet and not a record as defined in *Alberta Rules of Court* r 186[451]. The Calgary Health Region advanced several arguments in response. First, that each of the imaged hard drives was a single record as defined by *Alberta Rules of Court* r 186. Secondly and in the alternative, that even if the imaged hard drives were not records, their production was justified through the preservation and inspection provisions. Thirdly, it was impractical to segregate the relevant and irrelevant material, and fourthly, Innovative had through its pleadings, made the entire contents of the imaged hard drives relevant and material to the proceedings. Madam Justice Conrad referred to the case of *Lazin v Ciba-Geigy,*[452] where the court said that the plaintiff did not have to produce her entire diary for discovery as it contained both relevant and irrelevant material and only needed to disclose relevant parts. Similarly in *Royal Bank v Wallis,*[453] the court noted that a bank's book of accounts was not a 'document' but 'rather, it is a series of documents bound together for convenience.'

4.3.7 Storage Media - Conclusion

[4.3.7.1] As to the disclosure of hard drives and other media which comprise several items, sometimes even large volumes, of evidence, it is suggested that the approach of the Canadian courts is a sensible one. The questions remains whether Australian courts should take a similar approach when considering the admissibility of hard drives?

[4.3.7.2] In summary, the courts do recognise that electronic storage media can contain many documents. However, with respect, it appears that only the Canadian courts have made this distinction clear in the sense that there is a very definitive delineation between, say, a hard drive, and the documents contained upon it. The initial hurdle is for an applicant wanting access to a hard drive is to show that the documents stored upon the hard drive are relevant before a court will make an order for discovery or tender of that hard drive. Further, the Canadian courts recognise that an order may need to be made for an independent expert to examine the documents on the hard drive to ensure privileged, confidential and irrelevant materials is identified and separated out. While Australian courts and courts in the United States of America do recognise the privilege issues, it appears that there remains little guidance on how to deal with electronic documents stored on electronic media. It is generally when

[451] Canada, Courts of Alberta, *Alberta Rules of Court*.
[452] [1976] 3 W.W.R. 460 (Alta. S.C.(A.D.)), 66 D.L.R. (3d) 380.
[453] [1918] 2 W.W.R. 620, 13 Alta. L.R. 416, (1918) 41 D.L.R. 383.

dealing with electronic media that has been seized, that the courts talk about appointment of external experts to preserve privilege and confidentiality, and the courts have made it clear that there needs to be a specific process and reason when seizing records on a computer server because of the onerous burden being placed on the plaintiff.

4.3.8 Content

[4.3.8.1] If media which retains electronic documents is broadly defined as 'document', what about content? Print outs of computer information have certainly been held to be admissible.[454] However, what is the position concerning electronic documents in their 'native' format?

[4.3.8.2] The content of storage media may include files that are compressed repositories of files. For example, a forensic image may constitute one single file that requires specialist software in order to open that one file in order to gain access to a large volume of files contained therein. Likewise, an email repository may be in the form of a large compressed file, which once opened, contains may email message files and their attachments. None of the cases analysed appears to make this distinction and it is left to experts to deal with the various file types, compressed or otherwise. This type of content is best compared with database files, which have been considered by case law. These are examined further below in cases from Australia, the United States of America, England & Wales and Canada.

4.3.9 Content - Australia

[4.3.9.1] When considering content, the Federal Court of Australia came close to providing much needed analysis in the case of *Kennedy v Baker*.[455] There, the Federal Court considered whether the information stored in the hard drive of a personal computer is to be regarded as data from a single source, in the sense that it is a single thing constituted by a body of characters or symbols, or whether it is to be regarded as a collection of computer files each of which constitutes a source of data. The court concluded that a computer hard drive was a single source of data and, therefore, could be seized under the *Crimes Act 1900* (Cth) .[456] That

[454] *Regina v Spiby* (1990) 91 Cr App R 186 CA where computer recorded information about telephone calls was printed out and admitted into evidence.
[455] (2004) 207 ALR 247.
[456] *Kenned v Baker* (2004) 207 ALR 247 was applied in *Different Solutions Pty Ltd v Commissioner, Australian Federal Police (No 2)* (2008) 190 A Crim R 265; there the court acknowledged 'data' as a large body that

case involved seizure of evidence from hard drives pursuant to an amendment to the *Crimes Act 1900* (Cth) provided in the *Cybercrime Act 2001* (Cth). This amendment was intended to allow a forensic image of a hard drive to be made rather than have officers endeavour to locate evidence while conducting a search and seizure. Branson J concluded[457] that if the executing officer believes on reasonable grounds[458] that data from a particular source access by operating a computer might constitute evidential material, he or she may copy the data from that source to a disk, tape or other associated device brought to the premises.

[4.3.9.2] In arriving at her conclusion, Branson J noted from the explanatory memorandum circulated in respect of the *Cybercrime Bill 2001* (Cth) that previously only evidential material[459] could be copied. Given that a computer hard drive can hold large amounts of data, it is often not practicable for officers to search all of the data for evidential material while at the search premises, so allowing the whole hard drive to be imaged makes sense. While this conclusion, with respect, is the right one and is sensible in cases of seizure, again, the decision fails to clearly analyse the true nature of electronic documents, nor does it provide guidelines as to how non-evidentiary material is to be dealt with, once it has been obtained.[460]

encompasses computer files for the purpose of satisfying the definition of 'computer' in the *Crimes Act 1900* (Cth).

[457] Ibid at [66].

[458] Whether the Australian Federal Police can take a forensic image of an entire hard drive of a computer, will depend upon the search warrant and what constitutes 'reasonable grounds' pursuant to *Crimes Act 1900* (Cth) s 3L(1A). In *Zhang v Commissioner, Australian Federal Police* (2009) 260 ALR 580, the Federal Court granted an interlocutory injunction restraining the inspection of documents seized under search warrants. When searching computers, the search officers performed 'key word' searches, and if any of the key words were found on the computer, an image of the entire hard drive was taken. The Court held that *Crimes Act 1900* (Cth) s 3L(1A) may not clothe the Respondents with sufficient authority to copy the data on the disks in the manner in which they did, irrespective of whether 'data' is to be construed in the manner as concluded by Branson J in *Kennedy v Baker* (2004) 207 ALR 247.

[459] Whether electronic information has evidential value is important and is not a mere matter of labelling, it is a matter of substance. For electronic media to be seized and copied, it must be shown to contain evidential value: See *Hart v Commissioner of Australian Federal Police* (2002) 196 ALR 1; compare *Australian Federal Police v Carson* [2005] FCA 101 (11 January 2005) (Selway J).

[460] *Kennedy v Baker* (2004) 207 ALR 247, was distinguished in *ASIC v Rich* (2005) 220 ALR 324, [208] – [211] where the court ruled electronic evidence as admissible. There, the court determined that the Australian Federal Police ('AFP') were not authorised to make available to PriceWaterhouseCoopers' ('PwC') personnel 'things seized' under the search warrants. Notwithstanding that PwC was retained by ASIC to assist in the execution of the warrants and that some PwC personnel were deemed to be 'constables assisting' under the *Crimes Act 1900* (Cth) s 3C(1). However, 'things seized' which were made available to ASIC by the AFP could be made available by ASIC to properly appointed consultants, including PwC personnel, for the purpose of assisting ASIC officers in the performance of their functions and in the exercise of their powers. Provided that the ASIC officers retain supervisory control over the materials and discharge their statutory duty of confidentiality.

[4.3.9.3] *Kennedy v Baker*[461] defines a hard drive as data from a single source, and could be included as a decision under 'storage media' above. However, the inclusion of the words 'data from a single source' indicates that the court has given some consideration to the content that is contained upon storage media. However, with respect, the court does not provide this distinction, nor does it provide guidance of how to deal with the content of the hard drive.

[4.3.9.4] The content of a hard drive can comprise any number of formats. It can include email, which may be contained in an email repository, or emails may be individual files. The content may include word processing files created in Microsoft Word, spreadsheets contained in Microsoft Excel, or the content could be a database that has been created using proprietary software. In order to view any of these files, the content must be viewed with relevant software or processed with specialist software than is agnostic towards the software in which content was created. Either way, this is a salient point.

4.3.10 Content – England & Wales

[4.3.10.1] In England & Wales, an analysis of the case law regarding the content provides no more illumination than the cases regarding storage media. Earlier English cases have held that a database, whether stored in the computer itself or in backup files, so far as it contained information capable of being retrieved and converted into a readable form, is a 'document' and, therefore, discoverable.[462] No clear dividing line can be drawn between digital tape-recorded messages and the database of a computer on which information which has been fed into the computer is analysed and recorded in a variety of binary language.[463] Similarly, an earlier English decision found that databases, backup tapes and servers should be counted as documents and should be disclosed.[464]

4.3.11 Content – United States of America

[4.3.11.1] In the United States of America, there has been a plethora of decisions across the various jurisdictions that apply the definition of 'document' from the relevant legislation. The United States Court of Federal Claims has defined 'documents, data and tangible things' as 'to be interpreted broadly to include writings; records; files; correspondence; reports;

[461] (2004) 207 ALR 247.
[462] *Derby & Co Ltd and others v Weldon and others (No 9)* [1991] 1 WLR 652.
[463] Ibid applying *Grant v Southwestern and County Properties Ltd* [1974] 3 WLR 221.
[464] *Marlton v Tektronix UK Holdings Ltd* [2003] EWHC 383 (Ch).

memoranda; calendars; diaries; minutes; electronic messages; voicemail; E-mail; telephone message records or logs; computer and network activity logs; hard drives; backup data; removable computer storage media such as tapes, disks and cards; printouts; document image files; Web pages; databases; spreadsheets; softwares; books; ledgers; journals; orders; invoices; bills; vouchers; checks; statements; worksheets; summaries; compilations; computations; charts; diagrams; graphic presentations; drawings; films; charts; digital or chemical process photographs; video; phonographic tape; or digital recordings or transcripts thereof; drafts; jottings; and notes. Information that serves to identify, locate or link such material, such as file inventories, file folders, indices and metadata, is also included in this definition'.[465] This is a very broad definition, which covers all forms of electronic information.

[4.3.11.2] In the United States of America, similar to the position in Australia, merely copying the information does not constitute seizing.[466] Conversely, if the FBI accesses an internet account of a suspect and downloads files without obtaining a warrant, this would not be a seizure as it would not interfere with the defendant's, or anyone else's possessory interest in the data.[467] The use of a thermal imaging device from a public vantage point to monitor the radiation from a person's home constitutes a 'search' within the meaning of the Fourth Amendment and thus requires a warrant.[468]

[4.3.11.3] In courts in the United States of America, information held in databases can go beyond what is relevant to the case at hand, and allowing an adversary direct access to a database may allow them access to confidential information which could be prejudicial. While direct access to databases might be permissible in certain cases, there has to be a factual finding of non-compliance with the discovery rules. For example, in *Re: Ford Motor Company*[469] the appellant Ford Motor Company was granted a writ of mandamus ensuring that a discovery order was vacated. This discovery order had allowed the plaintiff direct access to the defendant's databases. While direct access might be permissible in certain cases, this would only permitted if there had been a factual finding of non-compliance with discovery rules, which did not exist in that case.

[465] *Pueblo of Laguna v US*, 60 Fed. Cl. 133 (2004).
[466] *Arizona v Hicks*, 480 U.S. 321, 107 S. Ct. 1149, 94 L. Ed. 2d 347 (1987).
[467] *United States v Gorshkov*, 2001 WL 1024026 (W. D. Wash. 2001).
[468] *Kyllo v United States*, 533 U.S. 27, 121 S. Ct. 2038, 150 L. Ed. 2d 94, 8 ILRD 37 (2001).
[469] 345 F.3d 1315, 1316 (11th Cir. 2003).

4.3.12 Content - Canada

[4.3.12.1] In Canada, the Ontario courts have held that an electronic database falls within the definition of 'document' within the relevant rules, but that a typical database would contain a great deal of information not relevant to the litigation.

[4.3.12.2] Like compressed files described above, databases are an interesting form of content. A database is generally software that stores information in a particular way. A piece of information stored as a field in a database is meaningless unless it is put into context with other pieces of information from the database. In order for the other fields of information to be pulled together, software is required in order to query the various database fields and present them as a report or other record. An example of this would be accounting software. The various pieces of financial information are stored as fields within the database and then at the end of each month after various manual entries have been completed, the software can produce reports such as profit and loss statements. To simply store each field of information in isolation from the software can render the information meaningless.

[4.3.12.3] In *Sourian v Sporting Exchange Ltd*,[470] the plaintiff requested production of a database report itemising all of the bets placed by a client who placed bets with Sporting Exchange and the IP addresses used by this client when those bets are made. The court considered the production of information from an electronic database and the challenges associated with such production. The court concluded that unless the entire database is produced together with any necessary software allowing the other party to examine its contents, what is produced is not the database but a database report organised in readable form. Accordingly, the court found that a database is not classified as a single document; rather a database report is discoverable. The court also noted that the court must consider whether production of a database report is more intrusive than producing the documents itself and have regard 'for how onerous the request may [be] when balanced against its supposed relevance and probative value.'

[4.3.12.4] Arguably, a database should be treated in the same way as a hard drive, in that some information is relevant, while other information may be confidential, irrelevant, privileged and so on. However, in order to obtain information from a database, generally, the

[470] 2005 CanLII 4938 (Ont. S.C.J.); 137 A.C.W.S. (3d) 712.

only way to obtain it, is to use the specialist software used to create and store the information, along with an expert, either agreed to by the parties or appointed by the court, who can use the software to produce the desired reports.

4.3.13 Content – Other Forms of Content

[4.3.13.1] Other forms of content include audio recordings such as telephone recordings, which have been held to be admissible as evidence.[471] Web pages create intricate issues, given that temporary copies can be created which may give rise to legal action.[472] Posts on social networking sites can be used as evidence, in a limited way, as long as it is relevant,[473] and instant messages have also been held to be admissible.[474] In *Re F.P.*,[475] court did not believe a whole new body of law was required to deal with new types of evidence such as emails or instant messages. The court held that the instant messages were properly authenticated based on the following factual circumstances: the defendant referred to himself by name, his testimony mirrored some of the comments in the instant messages, and he referenced one of the instant messages in a conversation with school authorities. Cookies, which are small files that store information related to a user's internet activity and provide reports back to the website that created the cookie, have been held to be admissible.[476] Likewise, chat room conversations

---

[471] *Addenbrooke Pty Ltd v Duncan (No 5)* [2014] FCA 625 (16 June 2014). See also *Grant v Southwestern and County Properties Ltd* [1974] 3 WLR 221, where a tape recording of a telephone conversation was held to be a discoverable document.

[472] In *Public Relations Consultants Association Limited v The Newspaper Licensing Agency Limited & Ors* [2013] UKSC 18, the Court considered whether copies of web pages created while internet browsing are exempt from copyright protection by reason of the 'temporary copies' exception provided by *Copyright Designs and Patents Act 1988* (Eng) s 28A. The case involved an appeal by Public Relations Consultants Association Ltd against a decision that a licence was required by its members to view media monitoring reports which were made available via a third party's website which monitored a large number of websites (Meltwater News).

[473] See *Giacchetto v Patchogue-Medford Union Free School Dist*., No. CV 11-6323(ADS) (AKT), 2013 WL 2897054 (E.D.N.Y. May 6, 2013), where the plaintiff sought damages as a result of being discriminated against on the basis of her disability. The defendant, the school, filed a motion to compel the plaintiff to authorise the release of records from her social media accounts, including Facebook, Twitter, and MySpace. The defendant argued that information from the plaintiff's social networking accounts were relevant to claims of physical and emotional damages, reflecting her social interaction, emotional and psychological state. The plaintiff objected to the motion on the basis that it was a 'fishing expedition' designed to impinge on her privacy. The Court found that the discoverability of the information was limited, holding that the fact that the information sought is an electronic file and therefore does not give the defendant the right to rummage through the entire file.

[474] In *Re F.P.*, 878 A.2d 91 (Pa. Super. Ct. 2005)., the defendant appealed from an assault conviction, asserting the trial court erred in admitting improperly authenticated computerised instant messages into evidence. The defendant argued the messages should have been authenticated by either the source Internet Service Provider or a computer forensic expert testimony. Rejecting this argument, the appellate court declared the instant messages admissible.

[475] *878 A.2d 91* (Pa. Super. Ct. 2005).

[476] See *Inventory Locator Serv., LLC v Partsbase, Inc.,* 2005 WL 2179185 (W.D.Tenn. Sept. 6, 2005) where the defendant offered 'Web server logs' purporting to record various unlawful entries into the defendant's computer system from an internet protocol ('IP') address assigned to the plaintiff. As evidence that the logs were altered

have been held to be admissible,[477] as are posts on social networking sites are also admissible.[478]

[4.3.13.2] In summary, while earlier cases were more inclined to admit electronic media into evidence, or make orders as to discovery of media, the courts do now appear to be recognising that such media contains a wide array of documents and information, which individually needs to be examined for discovery, including for privilege.

4.4 The Business Records Exception

[4.4.1.1] The Business Records Exception is one of the key exceptions to the Hearsay Rule. The rationale for the Business Records Exception is that businesses rely on certain records in day-to-day operations which give rise to level of trustworthiness,[479] and if records are created in the ordinary course of business, then they are likely to be reliable, and are fundamentally better than relying on people's memory:

> 'the law of evidence must be adapted to the realities of contemporary business practice. Mainframe computers, minicomputers and microcomputers play a pervasive role in our society. Often the only record of a transaction, which nobody can be expected to remember, will be in the memory of a computer. The versatility, power and frequency of use of computers will increase'.[480]

[4.4.1.2] In Australia, the *Uniform Evidence Acts* s 69 encapsulates the Business Records Exception. For the exception to apply, the document must form part of the records belonging to the organisation,[481] that the records are made in the course of business[482] and that the person admitting the documents has, or might reasonably be supposed to have had, personal

---

or fabricated, the plaintiff noted a 'cookie anomaly'. In response, the defendant submitted the affidavit from a technology services company president who explained the cookie anomaly as a technical glitch, not confined to entries from the plaintiff's IP address. Weighing this evidence, the court determined evidence exclusion was not warranted as '[a]bsent more detailed evidence or expert testimony', it could not determine if the 'cookie anomaly' undermined the authenticity of the defendant's log records.

[477] In *United States v Jackson*, 2007 WL 1381772 (D. Neb. May 8, 2007), an undercover police officer conducting the chat room conversation would cut-and-paste the entire conversation into a word document for later review. A computer forensics expert testified that this cut-and-paste method created several errors and that several portions of the defendant's conversations were omitted. The defendant argued the omitted portions of the transcript contained evidence relating directly to his intent and should not be admitted as evidence. The court found that the cut-and-paste document was not admissible evidence at trial because it was not authentic under the Federal Rules of Evidence.

[478] *Wesaquate v Steven Webb* 2012 SKQB 2 (CanLII) where McLellan J accepted that postings on web based networking sites such as Facebook are 'documents' and are therefore discoverable.

[479] *R v Lemay* (2004) 247 DLR (4th) 470 (British Columbia Court of Appeal).

[480] *R v Minors* [1989] 2 All ER 208.

[481] *Uniform Evidence Acts* s 69(1)(a).

[482] *Uniform Evidence Acts* s 69(1)(b).

knowledge of the asserted fact.[483] Further, the information can be directly or indirectly supplied by a person with knowledge of the asserted fact. [484] Other jurisdictions have similar provisions in their Evidence Acts. A summary of the relevant provisions throughout Australian jurisdictions is set out in Appendix 3.

[4.4.1.3] In England & Wales, hearsay has been abolished by the *Civil Evidence Act 1995* (Eng) s 1(1), although this Act has retained a number of relevant exceptions to the Hearsay Rule that still apply, including the Business Records Exception.[485] *Civil Evidence Act 1995* (Eng) s 9 provides that a document which forms part of the records of a business or public authority may be received in civil proceedings without further proof if a certificate is produced to the court and signed by an officer of the business or public authority. Likewise, *Criminal Justice Act 2003* (Eng) s 117 retains a statutory exception for documents created for business purposes.

[4.4.1.4] In the United States of America, the Business Records Exception is contained in *Federal Rules of Evidence* (USA) r 803(6). That rule provides that for the exception to apply, the record must be made by someone with knowledge,[486] the record was kept in the ordinary course of business[487] and that the making the record was a regular practice.[488] If those criteria are met, then neither the source of the information nor the circumstances of preparation indicate a lack of trustworthiness.[489]

[4.4.1.5] In Canada, the *Uniform Electronic Evidence Act* (Can) s 2(1) provides that the Act does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence. However, unlike the exceptions contained in legislation in other jurisdiction, the Canadian Act provides that 'the integrity of the electronic records system in which an electronic record is recorded or stored is presumed by evidence that supports a finding that the computer system was, at all material times, operating properly and if it was not operating properly then the integrity of the electronic record

[483] *Uniform Evidence Acts* s 69(2)(a).
[484] *Uniform Evidence Acts* s 69(2)(b).
[485] Pursuant to *Civil Evidence Act 1995* (Eng) s 1(1), evidence is not to be excluded in civil proceedings on the ground that it is hearsay. However, under section 4(1) it is for the court to decide 'the weight (if any)' to be given to any hearsay evidence.
[486] *Federal Rules of Evidence* (USA) r 803(6)(A)
[487] *Federal Rules of Evidence* (USA) r 803(6)(B)
[488] *Federal Rules of Evidence* (USA) r 803(6)(C)
[489] *Federal Rules of Evidence* (USA) r 803(6)(E)

was not affected, and there are no other reasonable grounds to doubt the integrity of the electronic records system.[490] Further the Act provides that the integrity of the electronic records system is presumed if it established that the electronic record was recorded or stored in the usual and ordinary course of business.[491]

4.5 Application of Business Records Exception

[4.5.1.1] The Hearsay Rule excludes the content of document, unless it is tendered through a witness, and the Business Records Exception allows records that are created in the ordinary course of business to be tendered through a person who has personal knowledge of the records. In this way, business records can be tendered into evidence without the need to have every person who created a record in an organisation appear in court to attest to the creation of the record. The result is a huge saving in court time. The Business Records Exception is a common sense once, however, the question for this thesis is whether the rules that have been developed over a long period, and that were developed for hard copy documents, are adequate to be applied to electronic documents, or whether the rule needs to be re-thought. There has been a sizeable increase in the computerisation of transactions in the course of ordinary business. Prior to the wave of computerised transactions, the commercial variables surrounding a purchase, such as cost, price, and quantity were separately considered prior to completing an actual market transaction. Today, the majority of commercial transactions are carried out in electronic form, proving a comprehensive electronic record of the transaction. This has vastly increased the volume of data available for analysis in a wide range of cases.[492]

[4.5.1.2] As early as 1940, the High Court recognised that common sense dictated that books of account kept according to an established system in an organised business, were receivable in evidence as proof, despite there being little English authority explaining why this is so.[493] By as late as 1965 however, *Myers v Director of Public Prosecutions*[494] remained the leading English authority for the requirement that unless the maker of the records was deceased, they had to be identified and appear in court to speak to the evidence.

[490] *Uniform Electronic Evidence Act* (Can) s 5(1)(a).
[491] *Uniform Electronic Evidence Act* (Can) s 5(1)(c).
[492] Lewis Evans, 'Economic Measurement and the Authorisation Process: The Expanding Place of Quantitative Analysis' (1999) 13 *Competition and Consumer Law Journal* 99.
[493] *Potts v Miller* (1940) 64 CLR 282.
[494] [1965] 1 AC 100.

[4.5.1.3] In Australia, the courts are willing to accept that although mistakes may occur in the making of business records, they occur less often than in the recollection of persons trying to describe what happened at some point in the past.[495] However, mistakes do occur and it has been suggested that verbal assurances that audits take place and systems are secure are regularly accepted into evidence.[496]

[4.5.1.4] The Business Records Exception was considered at length in the case of *ASIC v Rich,*[497] with regards to ten categories of documents largely collected from the computer systems of One.Tel, which were seized by the liquidators when that company went into liquidation. These documents included business plan summaries, budgets, trial balances, management accounts, bill run breakdown, spreadsheets relating to gross margin, Australian collections profile summaries, liquidators' reports to creditors, an email and a butcher's paper presentation relating to billing. Austin J held that all the categories of documents were admissible evidence under the Business Records Exception. In coming to his conclusion, Austin J took into account a number of factors, including the footers on the document indicating their character as management accounts and the fact the documents were located in the finance directory on the servers, which indicated their character as management accounts. Despite an argument by ASIC that the 'modified' dates being later than the asserted dates, His Honour said these were anomalies, which if not explained by other evidence, would affect, and possibly destroy, the probative value of the documents, but that does not go to authenticity.[498] Austin J in *ASIC v Rich,*[499] held reports were records just as copies of letters to the creditors also constituted business records for a liquidation firm. His Honour analysed the case law in relation to the authentication of documentary evidence, including business records, and this analysis is set out further in section 6.5.

[4.5.1.5] Magazines and promotional journals have been held not to be 'business records' such that they will not fall within the Business Records Exception. In *ACCC v Air New Zealand*

[495] *Albrighton v Royal Prince Alfred Hospital* (1980) 2 NSWLR 542.
[496] Maryke Silalahi Nuth, 'Unauthoized Use of Bank Cards With or Without the PIN: A Lost Case For The Customer?' 9 *Digital Evidence and Electronic Signature Law Review* (2012) 95-101 and Journal number 04-016794TVI-TRON, *Bernt Petter Jǿrgensen v DnB NOR Bank ASA by the Chairman of the Board* (Trondheim District Court, 24 September 2004), 9 *Digital Evidence and Electronic Signature Law Review* (2012) 117-123.
[497] (2005) 216 ALR 320.
[498] Ibid [40].
[499] (2005) 216 ALR 320.

Limited (No 5),[500] Perram J consid**e**red the question of whether magazines and promotional journals were 'business records'. He referred to the earlier case of *Roach v Pages (No 15)*[501] in which an extract from the 'Australian Mushroom Growers' Association Journal' was rejected as a business record on the basis that there is a distinction between 'documentary products of a business (such as magazines and journals) and records which record the business activities.' The underlying foundation behind this distinction is that records of business activities are likely to be correct, whereas the same cannot be said with regards to publications such as advertising or public relations pieces. In the later case of *Roach v Pages (No 27),*[502] Sperling J also rejected an application that website material be accepted under the Business Records Exception.

[4.5.1.6] Email has been held to constitute a record of business. In *Australian Competition and Consumer Commission v Air New Zealand Limited (No 1),*[503] Perram J held that 'an email system is built on a highly formalised file system, all the communications which take place over it are kept, at least for some time, and often permanently. In that sense they are records and, where an email system is maintained by a firm, it is natural to see the records thus maintained as records of that business'.[504] Representations within multiple email chains have been held to be admissible pursuant to the Business Records Exception.[505]

[4.5.1.7] However, it is worth noting that outside of the *Uniform Evidence Acts*, a party may also rely on *Corporations Act 2001* (Cth) s 1305 which provides that a book kept by a body corporate pursuant to the Act is admissible in evidence in any proceeding and is prima facie evidence of any matter stated or recorded in the book.[506]

[4.5.1.8] In England & Wales, business records can be admitted without the need to call

[500] (2012) 301 ALR 352.
[501] [2003] NSWSC 939 (20 October 2003).
[502] [2003] NSWSC 1046 (13 November 2003).
[503] (2012) 301 ALR 326.
[504] Ibid [57].
[505] *Addenbrooke Pty Ltd v Duncan (No 5)* [2014] FCA 625 (16 June 2014). Foster J considered whether the representations made in an email chain were made by a person who had or might reasonably be supposed to have had personal knowledge of the asserted facts, pursuant to *Evidence Act 1995* (Cth) s 69(2)(a), in order to disregard the principle objection that the representations contained in those documents are hearsay and are not rendered admissible by the application of any of the statutory exceptions to the Hearsay Rule, pursuant to s 59. Foster J commented that there was no dispute that the print out of the email chain was a document which forms part of the records belonging to or kept by the company in the course of, or for the purposes of, its business; at [45].
[506] *Corporations Act 2001* (Cth) s 1305(1).

the maker of the record.[507] Moreover, documents have been implied to include electronic documents in orders made by the court. In *Daltel Europe Ltd &Ors v Makki & Ors*,[508] the court orders required the delivery of a wide range of records, which included digital records, and made a provision for documents on the computers accessible from Mr Makki's office and home to be both copied and inspected. Interestingly, this case adopted a flexible approach to hearsay in relation to electronic evidence.

[4.5.1.9] In the United States of America, initially in the late 1990's a number of courts held that emails did not constitute a written document. However in the 2005 in the case of *International Casings Group Inc v Premium Standard Forms*,[509] the court held that a string of emails between parties' could be read to infer an agreement and the emails could be read together to locate all the terms of the contract. The Supreme Court of the United States of America has held a tape recording to be admissible, despite the person whose voice was recorded on the tape giving evidence.[510] This has led to some uncertainty regarding the scope of admissible hearsay in criminal trials.

[4.5.1.10] Canadian courts have recognised that business records are generally accurate and that is not generally required for the admission of business records to have a live witness attest to the accuracy of the system that creates and stores the records. Rather, the 'circumstantial guarantee of trustworthiness inherent in such records, such that they can be admitted as an exception to the Hearsay Rule, arises from the assumption that companies would not establish record-keeping systems that were not accurate.'[511] Chasse[512] argues that the most serious failing of the business record provisions in the Canadian Evidence Acts are that (a) they fail to inform adequately as to what evidence is needed for proof of the truth of business records sufficient to render them admissible in evidence; and (b) they allow court decisions to ride off in all directions because the tests they provide are undefined and too vague to command

[507] *Brown v Secretary of State for Social Security* (1994) Times Law Reports, 7 December; *R v Derodra* [2000] 1 Cr App Rep 41; *Vehicle and Operator Services Agency v George Jenkins Transport* [2003] EWHC 2879 (Admin).
[508] [2006] 1 WLR 2704.
[509] 358 F.Supp.2d 863 870-72 (W.D. Mo. 2005).
[510] *Crawford v Washington* (2004) 541 U.S. 36.
[511] *R v Marini* 2006 CanLII 34282 (ON S.C.) [43].
[512] Ken Chasse, 'Electronic Records as Documentary Evidence' (2007) *Canadian Journal of Law and Technology*, 141, 156.

consistency in judicial interpretation.[513]

[4.5.1.11] In summary, it appears that the courts are applying the Business Records Exception to electronic documents, in the same way as they would apply the rule to hard copy documents, without any further test or examination. This requires further exploration as to whether electronic documents are being sufficiently authenticated, and this is addressed further in Chapter 5.

4.6 Business Records – A Practical Consideration

[4.6.1.1] Any analysis of the law about documentary evidence is not complete unless a review of the way in which documents are created and stored by businesses is reviewed as well. The vast majority of businesses no longer have a document retention policy that reflects what happens in practice. The *Electronic Transactions Acts* provide for retention of records in an electronic format.[514] However, electronic records are so easy to store and storage media are relatively inexpensive, the reality is that businesses simply store huge volumes of documents randomly, and this is increasing each year. When a business has to locate and retrieve documents to be used in evidence, it has to do so in a cost effective way. This presents a challenge where there is no proper archiving system.

[4.6.1.2] Although technology is making it easier to store vast quantities of documents, the converse is that technology is also making it easier to search and retrieve relevant evidence where there is an orderly system of storage in operation.

[4.6.1.3] Standards for record keeping are set out in AS ISO 15489.1. AS/NZS ISO/IEC 17799:2001 Information technology sets out a Code of Practice for information security management, and provides that information classification requires organisations to develop an information classification scheme that indicates the need, priorities and degree of protection and label electronic records accordingly. An organisation's information classification and labelling scheme must include an assessment of the potential evidentiary significance of electronic records. HB171-2003 outlines standards for the preservation of evidence and the

[513] Ibid 147.

[514] *Electronic Transactions Act 1999* (Cth) s 12, *Electronic Transactions Act 2000* (NSW) s 11, *Electronic Transactions Act 2000* (Vic) s 11, *Electronic Transactions Act 2001* (Qld) s 20, *Electronic Transactions Act 2000* (SA) s 11, *Electronic Transactions Act 2011* (WA) s 12, *Electronic Transactions Act 2000* (Tas) s 9, *Electronic Transactions Act 2001* (ACT) s 11, *Electronic Transactions Act* (NT) s 11.

obligation to provide records which includes (a) understanding regulatory, administrative and best-practice obligations to produce, retain and provide records; (b) understanding the steps that can be taken to maximise the evidentiary weighting of records and the implications of not doing so; and (c) understanding regulatory constraints to the retention and provision of records. A suggested design for evidence is set out in the Standard so that computer systems and procedures are capable of establishing the following:

(a) The authenticity and alteration of electronic records;
(b) The reliability of computer programs generating such records;
(c) The time and date of creation or alteration;
(d) The identity of the author of an electronic record; and
(e) The safe custody and handling of records.

[4.6.1.4] This applies to the design or acquisition of new systems or the upgrade of existing systems. The Standard provides that organisations must ensure that records are stored in a format that is useable in the future. The timeframe to be considered will be based on the record's classification and labelling and is particularly important when computer systems are upgraded or changed.

[4.6.1.5] To establish the authenticity of electronic records, there are generally two steps (a) identifying the original electronic record; and (b) identifying alteration.

[4.6.1.6] Organisations must be able to establish that a particular electronic record has not been altered. This can be achieved by (a) retaining the original document in non-electronic form; (b) relying on computer operating system facilities and circumstantial evidence; (c) storing the original electronic record or a validated copy on write once read many (WORM) media; or (d) using cryptographic techniques (eg hash or MAC).

[4.6.1.7] The Standard provides that in many situations, records will be admitted with significant evidentiary weighting even though minor changes have occurred, so long as those changes are 'immaterial' and arise in the normal course of communication, storage or display. In such cases, organisations must be able to demonstrate that the immaterial changes have not changed the substantive content of the record. In some situations, it is sufficient to demonstrate that only authorised persons or programs have access to create or alter the electronic record. In such cases, the organisation must be able to demonstrate that (a) unauthorised persons or programs are prevented from altering the electronic record; and (b) authorised persons or programs did not alter the electronic record.

[4.6.1.8] Computer system access controls restrict unauthorised persons or programs from accessing and altering an electronic record. AS/NZS ISO/IEC 17799:2001 (Code of practice for information security management) sets out best practice for information security access controls.

[4.6.1.9] The reliability of a computer program can be established by expert analysis of the source code. Organisations that produce their own software, or use open-source software, should retain the source code for computer programs and be able to demonstrate that the computer program was in fact generated from the particular source code. Organisations that purchase software should obtain the source code, or alternatively ensure that the manufacturer retains the source code for the particular version of the program that is used.

4.7 Summary & Conclusion

[4.7.1.1] The case law reviewed in this Chapter 4 serves to highlight the inconsistent way in which electronic information is treated as evidence before the courts, particularly documentary evidence. The definition of 'document' as defined in the various Evidence Acts is set out in section 4.2, and how this is applied to electronic documents, has been examined above in section 4.3.

[4.7.1.2] Prior to electronic information being used as documents, if one was asked to describe a 'document', then one would have answered that a document is a flat piece of paper on which there is written some sort of information. The definition might have included a medium other than paper, such as a sign, gravestone and so on. When electronic media came into common business usage, then rightly, the definition was broadened to extend to these new types of media.

[4.7.1.3] However, is the definition too broad? The courts are right to include all forms of media as 'documents' when the definitions are as broad as they are. The fact they are so broad does, it is suggested, cause problems which distort the common understanding of what a document actually is. In *Sony BMG Music Entertainment v Arellanes*,[515] the argument that a CD-Rom was not a document per se, but rather, a repository of several different documents, was put to the court. This argument was rejected by Tamberlin J in that case, as his Honour

[515] 2006 U.S. Dist. LEXIS 78399 (E.D. Tex. Oct. 27, 2006).

confirmed that the definition of 'document' in the *Uniform Evidence Acts* was indeed broad enough to cover the CD-Rom itself. It is suggested, with respect, that this conferral of devices as a 'document' rather than a repository of documents, much like a filing cabinet full of pieces of paper, is with the greatest of respect, a flawed application of the word 'document', and has led to problems and misunderstandings in the use of electronic media. A hard drive can contain millions of 'documents' including irrelevant, privileged and confidential documents to which that the other party should not be privy. The courts have dealt with this in a haphazard and inconsistent way by allowing independent experts to review material of these drives in order to assist with the determination of privileged material. The issue with engaging independent third parties is that there is invariably a not insubstantial cost involved, and that the third party needs to make these determinations in isolation of the issues dear to the respective party involved. Additionally, the third party expert is invariably not a lawyer and not across the rules of evidence. Issues to consider with such appointments is who appoints the third party, and ensuring they are truly independent of the parties. With respect, it is the Canadian courts which have most clearly articulated the issue, defined the problem and provided a solution.

[4.7.1.4] If each 'document' on a hard drive is treated as if it were a paper document, each document can be dealt with adequately in terms of privilege, discovery and ultimately as evidence before the court. What of databases that can only be examined utilising the software used to create the database, and what of reports that are generated using that software? First, there needs to be an understanding that a database is a collection of information that can be queried to produce a report, which then becomes a document in the ordinary sense of the word. The information stored in a database is unintelligible to the ordinary user on its own, the database requires software to read and interpret the data stored within the various tables, and it requires a report to be generated in order for a user to view and understand the data. Of course, various reports can be produced, depending upon the way in which the database is queried. As explained in section 3.6.7, a database stores records in a tables, and the contents of the tables can be reproduced in reports. Calculations can also be conducted on the tables, with results shown in the report generated. To demonstrate how a document is produced, one would need a witness to explain how the calculations are made in order to explain what the output means. In some cases, the software producing the reports may be quite well known, such as Microsoft Excel, however, if bespoke software has been developed, the software developer may be called to explain how calculations are made. This highlights the very difference between paper

records and electronic records.

[4.7.1.5] Before examining the rules of authentication of documentary evidence and how these rules are applied in Australia to electronic evidence, it is necessary to review how electronic evidence is collected and whether there are any rules that need to apply to the preservation of electronic evidence as compared with paper. The process of locating evidence to be produced to a court is through discovery or disclosure. The rules of discovery or disclosure necessitate further examination of how documents are treated by the courts, and the process of discovery also determines whether a document is relevant or not. Of course, if a document is not relevant, then it is generally not admissible, and would not need to be authenticated.

[4.7.1.6] The other principal characteristic of admissibility of evidence is that it is capable of authentication. This aspect is next considered in relation to electronic evidence.

[4.7.1.7] The questions that arise from an analysis of the rules of documentary evidence, as they apply to electronic evidence, are:

Question 2:
Is the definition of 'document' in the *Uniform Evidence Acts* adequate for the purposes of electronic evidence and, in particular, does it appropriately identify the nature of electronic evidence in that it comprises both content and storage media?

Question 3:
Should the Business Records Exception, in its present for in the *Uniform Evidence Acts*, continue to apply to electronic evidence, or does it need modification?

5. CHAPTER 5 – DISCOVERY / DISCLOSURE OF ELECTRONIC EVIDENCE

[5.1.1.1] Only evidence that is relevant and authentic may be tendered in proceedings. To be authentic, evidence must be what it purports to be, with 'integrity' being a key attribute of authenticity.[516]

[5.1.1.2] Before considering the issue of authentication, documentary evidence often has a long journey from its collection to presentation in court. With electronic evidence, this process is much more complex and involved than evidence in paper form. Historically, with paper, either the original document was tendered, or a copy which the court was satisfied by various means, was indeed a copy of that original. With electronic documents, it is difficult to prove which 'document' is the 'original' since two electronic documents can be identical. If they are authenticated using the 'MD5 hash algorithms' further described in section 3.3.3. Indeed, the entire concept of 'original document' is not apposite to describe electronic documents.

[5.1.1.3] The authenticity of a document may be called into question during one of the steps on the path to trial, therefore, each of these steps are considered in detail below.

(a) Identification, Preservation & Collection of Electronic Evidence
(b) Processing, Reviewing and Analysis of Electronic Evidence
(c) Identifying Privileged evidence
(d) Producing Electronic Evidence
(e) Presenting Electronic Evidence in Court

[5.1.1.4] If discovery orders are made, then items (a) to (c) are part of the Discovery process, which is described further below in sections 5.2 to 5.5.

5.2 Identification, Preservation & Collection of Electronic Evidence

[5.2.1.1] Once an electronic document is admitted into evidence, the court uses two criteria to measure its evidentiary weight. The first is probative value, which is, whether the electronic record is relevant and whether authorship and authenticity have been established. Secondly, whether the electronic record been collected and handled correctly and in accordance with these rules?[517]

[516] Paul, *Foundations of Digital Evidence*, above n 25, 36.
[517] Dahiya & Sangwan, above n 24, 24-25

[5.2.1.2] Unless the evidence is collected in such a way that the chain of custody is preserved from the time of collection until presentation at trial, this may affect admissibility or if admitted, the weight that the court may attach to the evidence. To obviate this challenge, a specialist, evolving, 'science' has emerged to assist the court, known as 'computer forensics'. Computer forensics encompasses four elements: identification, preservation, analysis and presentation. Safeguards and methodologies used by computer forensics experts must preserve evidence in a way that will withstand both judicial scrutiny and that an opposing party, should the matter go to trial. Therefore, copies of original electronic data are used for analysis. This ensures that the original electronic evidence can be protected from accidental damage or unintentional alternation.

[5.2.1.3] When gathering evidence, the first task is to identify which documents are to be collected, and this can be assisted by answering the following questions:

(a) What evidence is required? - What type of evidence needs to be collected, including hard copy, electronic evidence and real evidence?
(b) Where is the evidence? - Electronic evidence can be located in a number of disparate locations as specified in Chapter 3.
(c) When are the relevant periods? – The periods during which the issues in the matter occurred will be relevant.
(d) Whose data is relevant? – Only certain people's evidence may need to be collected.
(e) How will the data be collected? – Will expert assistance be required to collect the data?

[5.2.1.4] Any collection of electronic evidence should be done in a forensically sound manner, where possible,[518] that is, firstly, it's meaning and therefore, the interpretation of the electronic evidence has been unaffected by the computer forensic process. Secondly, all errors must be reasonably identified and satisfactorily explained so as to remove any doubt over the reliability of the evidence. Thirdly, that the way in which the evidence was collected is transparent, that is, the electronic process is capable of being independently examined and verified in its entirety. Finally, the computer forensic analysis must be undertaken by an individual with sufficient and relevant experience.

[5.2.1.5] When duplicating evidence, the original data needs to be handled in a forensically sound manner from the time it is initially copied until it is presented in court. The chain of custody needs to be assured by appropriately qualified experts. The duplication

[518] Rodney McKemmish, 'IFIP International Federation for Information Processing' (2008) 285 *Advances in Digital Forensics IV* 3.

process must produce an accurate and reliable reproduction of the original and failure to do so may result in invalidated results. Any duplication process requires the computer forensics expert to use methods and applications that assure the duplicate image will produce an output that matches the original. The traditional method of forensic collection is by using a process known as 'forensic imaging'.[519] This is the process of creating an exact bit-for-bit replica of the data stored on an original electronic medium. A benefit of taking a bit-for-bit copy is that all data on the medium is copied, including data which resides in unallocated space, or in 'file slack'; often 'deleted' files are retained in the file slack. The original medium can then be secured and the copy used for forensic analysis. The imaging process can be verified using a hash algorithm such as MD5 or SHA-1 which can be used to determine if the image has been tampered with (if the MD5/SHA-1 is different to the one taken at the time the image is made, this is an indication that the image has been changed or altered). Any forensic collection of electronic evidence should be done in accordance with industry standards and principles,[520] and the data should be captured in accordance with an established and maintained quality assurance system.[521] A forensic copy of the original evidence should be made for working purposes, so the original can be secured and remain untouched and any examination is best conducted on a copy of the original evidence. The forensic examiner may be required to give evidence of how they have handled the evidence and may have to show that the evidential

[519] The safest way to forensically preserve digital evidence is to engage a qualified computer forensics expert because no one is better equipped to prevent problems or resolve them should they arise. Taking a duplicate copy of active data means that only file copies can be made, and a forensic image is unable to be made. A forensic image can only be made where all information on the media can be preserved.

[520] The National Institute of Justice US published a report in 2004: Forensic Examination of Digital Evidence: A Guide for Law Enforcement, United States National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (2004) <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf> at 11 September 2015, that agencies can use to help them develop their own policies and procedures. When dealing with digital evidence, general forensic and procedural principles should be applied and actions taken to secure and collect digital evidence should not affect the integrity of that evidence. Persons conducting an examination of digital evidence should be trained for that purpose. The activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review. Digital evidence is fragile and can be altered, damaged, or destroyed by improper handling or examination.

[521] There should be up-to-date standard operating procedures which are supported by proper case records and broadly accepted procedures, equipment and materials which are reviewed regularly. Procedures should be used which are generally accepted in the field or be supported by data gathered and recorded in a scientific manner. The hardware and software used should be up-to-date and reliable. Any action that has the potential to alter, damage, or destroy any aspect of the original evidence must be performed by appropriately qualified persons in a forensically sound manner. Written records should be kept of all activity to preserve the chain of custody, that is, who handled what at each stage of evidence handling. All activity in relation to the gathering of evidence should be recorded in writing and be available for review and testimony. All evidence should be clearly labelled, including whether media are originals or copies; the current date and time should be noted on the label, as well as the name and initials of the person who made the copy, as well as the name of the operating system used, the command that was used to copy files and the information believed to be in the files written copies of appropriate technical procedures should be maintained.

integrity remains intact. However, there are no rules of court that provide for this, and remains in the realm of expert witnesses.

[5.2.1.6] Since the advent of Cloud Computing, where server space is 'rented' on a virtual computer, a forensic image of the hard drive may not be possible, because it is not possible to do so on a virtual computer (an explanation of Cloud Computing is set out further in section 3.5.8). In the case of collecting evidence stored in the Cloud, the first port of call is to request the login details to the server. Without these, it can be difficult to access the information, because there may first be questions of custody and control to address. Thus, for the evidence to be admissible, some form of certification of capture and storage by a qualified expert should be tendered to the court with the electronic evidence.

5.3 Discovery or Disclosure

5.3.1 What is Discovery/Disclosure?

[5.3.1.1] Discovery/disclosure is part of the litigation process in collecting evidence, therefore, if evidence is to be authenticated, the discovery process should aid authentication. Discovery is also known as 'disclosure' in some jurisdictions, however, for the sake of consistency, it will be referred to throughout as 'discovery',

[5.3.1.2] Discovery should be limited to documents that can prove the issues narrowed by the pleadings.

[5.3.1.3] Historically, discovery originated in the ecclesiastical courts and Chancery in England. Common law courts could not order discovery until statutory reforms gave that power in the 19th Century, therefore, the basis for discovery is equitable and it is a substantive right in equity. The principles of equity permitting discovery apply where the rules governing litigation are silent.[522]

[5.3.1.4] The basis of modern common law process of civil discovery is given by Lord Donaldson MR in *Davies v Eli Lilly & Co.*[523] His Lordship said:

> [L]itigation in this country is conducted 'cards face up on the table'. Some people from other

[522] Andrew Combe, *Young Lawyers Seminar on Discovery*, Third Floor Wentworth Chambers <http://3wentworth.com.au/wp-content/uploads/2012/06/Young-Lawyers-Seminar-on-Discovery.pdf> at 11 September 2015 [2].
[523] [1987] 1 WLR 428.

> lands regard this as incomprehensible. 'Why', they ask, 'should I be expected to provide my opponent with the means of defeating me?' The answer, of course, is that litigation is not a war or even a game. It is designed to do real justice between opposing parties and, if the court does not have all the relevant information, it cannot achieve this object. [524]

[5.3.1.5] Discovery assists the parties to prepare for trial, by allowing relevant evidence to be collated, documented and exchanged with the other parties to the matter. The process of undertaking discovery is outlined in each jurisdiction's Rules of Court, and lists must be prepared and exchanged in the prescribed format, within the period permitted by the Rules of Court. If evidence is stored in records management systems, the parties should be mindful of authentication requirements during discovery.[525]

[5.3.1.6] If documents are not collected in a way that preserves their integrity, they may be at risk of not being admitted in evidence at the hearing. Further, at the initial stages, objections to disclosure may be considered and any documents that attract legal professional privilege, need to be considered and properly identified. This section 5.3 outlines the discovery process and how document evidence is collected, analysed, reviewed, exchange and ultimately presented as evidence in court.

[5.3.1.7] Many courts, including the Jackson Civil Procedure Reforms in the United Kingdom,[526] are now critical of the current discovery process, saying that it increases costs to the litigant and in many cases, is unnecessary. Indeed, the Equity Division of the Supreme Court of New South Wales only allows discovery where an order of the Court has been made.[527] That Court instead, insists upon the parties first preparing and filing their witness statements and affidavits, prior to any discovery order being considered. Of course, where the parties can show that discovery is necessary for the case, then that argument can be put to the court and appropriate orders can be made.[528]

5.3.2 What is Electronic Discovery?

[5.3.2.1] Electronic discovery is the process of discovering documents that are in electronic format. Electronic documents are either hard copy documents converted to an

[524] Ibid [805].
[525] The Sedona Conference, *Commentary on Evidence & Admissibility*, (March 2008) <http://www.thesedonaconference.org> at 11 September 2015, [2].
[526] Lord Justice Jackson, Review of Civil Litigation Costs: Final Report, 21st December 2009.
[527] Australia, Supreme Court of New South Wales, *Practice Note SC Eq 11*, 22 March 2012.
[528] Ibid.

electronic format, including capture of metadata or electronic documents in their 'native' format (that is, in their original format). Metadata is an essential component of electronic documents and printing out electronic documents to review them can mean critical metadata may be missed and it can be difficult to cross-reference back to the original files if some form of unique identification has not been undertaken.[529]

[5.3.2.2] Electronic discovery can be as simple as the preparation and exchange of a spreadsheet and images, through to the exchange of a database and images/files. A spreadsheet is a simplified version of a database and means that if discovery is to occur electronically, the individual components of each document are already captured in a structured way, enabling the data to be imported into a database.

[5.3.2.3] Questions of legal professional privilege must be considered in the same way as non-electronic discovery.

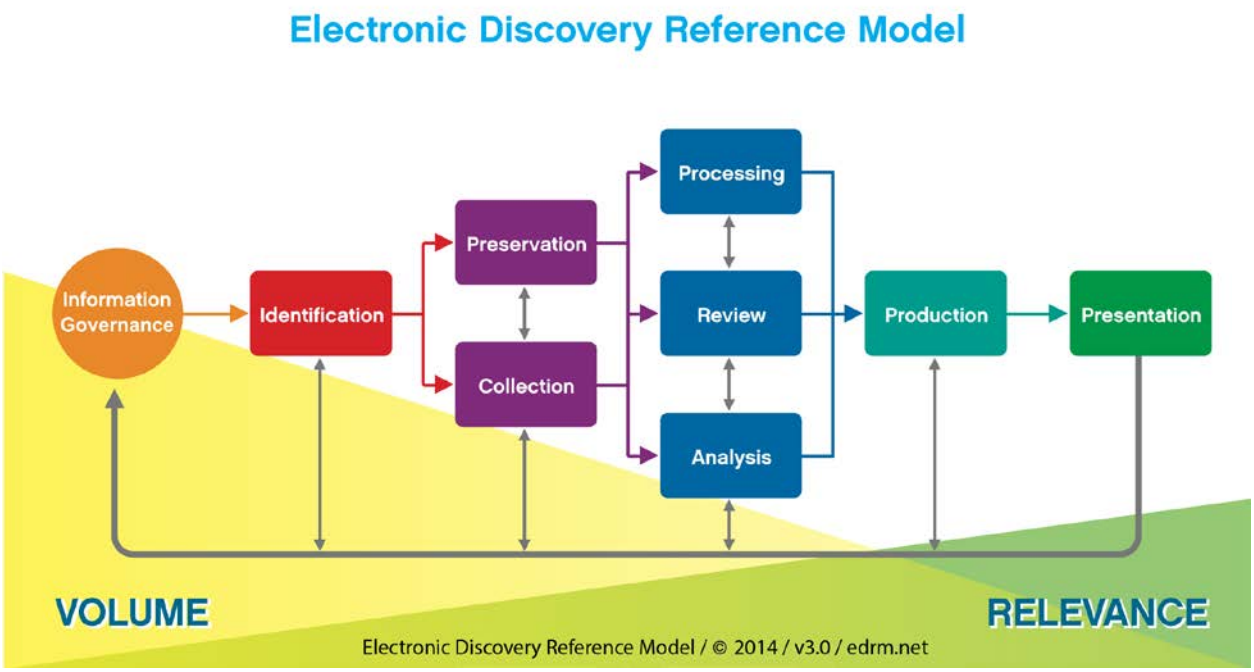
5.3.3 Standards for Electronic Discovery

[5.3.3.1] Given the unique nature of electronic documents, electronic discovery is now an industry in its own right. As a result, standards are being developed so that discoverable electronic documents are prepared and exchanged in a consistent format during discovery and this ultimately will mean cost and time savings for the litigants. It also means a great deal of care is taken to ensure electronic evidence is not changed. An electronic discovery reference model ('EDRM') has been developed and is used as a basic tool for the identification, collection, analysis, processing and presentation of electronic evidence. Shown below, the EDRM model is now considered an international standard. [530]

[529] Pontello M., *TrIDEngine* (2012) Marco Pontello's Home Page <http://mark0.net/code-tridengine-e.html> at 11 September 2015. File header analysis should be conducted on files in order to authenticate what format files really are. File header analysis software uses a match-rating scale, so if the file is assessed as matching one type, but may match another type as well, the rating which scores the highest will be the file type assigned to the file.

[530] Refer Electronic Discovery Reference Model website: <http://www.edrm.net/> at 11 September 2015.

Figure 1: Electronic Discovery Reference Model



[5.3.3.2] This figure shows how as documents progress through the e.discovery process, from identification through to presentation in court, as the volume of documents increase, the relevance will increase. Information Governance was added to the EDRM in 2014, as organisations start to value the importance of storing electronic information in such a way that documents relevant to the issues in a dispute can be easily located and retrieved.

[5.3.3.3] The EDRM was created in May 2005 to address the lack of standards and guidelines in the e.discovery industry, a problem that had previously been identified in the 2003 and 2004 Socha-Gelbmann Electronic Discovery surveys as a major concern for consumers and providers alike.[531] EDRM is continually updating and expanding the original model and now includes six projects in total, including the EDRM. The other five projects are the Computer Assisted Review Reference Model (CARRM), the Information Governance Reference Model (IGRM), the Metrics Model, the Privacy Risk Reduction Model and the Talent Task Matrix. The overriding purpose of the Model is to ensure that the evidence is not lost or tampered with pending trial.

[531] Socha G. & Gelbman T., *EDRM Stages* (2014) The Electronic Discovery Reference Model <http://www.edrm.net/resources/edrm-stages-explained> at 11 September 2015.

5.3.4 Court Rules, Practice Notes and Protocols for e.Discovery

[5.3.4.1] Almost all Australian jurisdictions have practice notes on the use of technology in civil litigation.[532] *The Federal Court of Australia Practice Note CM6*[533] and the *Supreme Court of New South Wales Practice Note SC Gen 7*[534] deal with electronic documents in their native format, whereas practice notes from other jurisdictions are primarily concerned with converting hard copy documents into an electronic format, most commonly, by imaging hard copy materials and manually capturing objective data about each document (which is a different process).

[5.3.4.2] Other jurisdictions such as England & Wales[535] and Canada[536] are implementing similar practice directions. In the United States of America, the *Federal Rules of Civil Procedure* (USA)[537] have been amended to incorporate guidelines developed out of the Sedona Conference.[538] In Canada, the Ontario Bar Association have Electronic Discovery

[532] Australia, Federal Court of Australia, Practice Note CM6 *The Use of Technology in the Management of Discovery and the Conduct of Litigation*, 29 January 2009, Federal Court website: <http://www.fedcourt.gov.au> at 11 September 2015; Australia, Supreme Court of Queensland, Practice Direction 2011/10 – Use of Technology for the Efficient Management of Documents in Litigation, Supreme Court of Queensland website: <http://www.courts.qld.gov.au> at 11 September 2015; Australia, Supreme Court of New South Wales, SC Gen 7 *Supreme Court – Use of Technology*, 9 July 2008, commenced 1 August 2008, Supreme Court of New South Wales website: <http://www.lawlink.nsw.gov.au> at 11 September 2015; Australia, Supreme Court of Victoria, Practice Note, No 1 of 2007 *Guidelines for the Use of Technology in any Civil Matter*, Supreme Court of Victoria website: <http://www.supremecourt.vic.gov.au> at 11 September 2015; Australia, Supreme Court of South Australia, *Supreme Court Civil Supplementary Rules 2014* (SA), Chapter 7 Part 3, Division 2 deals with electronic disclosure in basic form and Chapter 7 Part 3 division 3 deals with electronic disclosure in advanced form, Supreme Court of South Australia website: <http://www.courts.sa.gov.au> at 11 September 2015; Australia, Supreme Court of the Northern Territory, Practice Direction No 2 of 2002, '*Guidelines for the Use of Information Technology in any Civil Matter*, 13 February 2002, Supreme Court of the Northern Territory website: <http://www.supremecourt.nt.gov.au> at 11 September 2015; Australia, Supreme Courts and District Courts of Western Australia *Technical Guide for Preparing and Submitting Documents for E-trials*, 24 September 2008, Supreme Court of Western Australia website: <http://www.supremecourt.wa.gov.au> at 11 September 2015.

[533] Australia, Federal Court of Australia, Practice Note CM6 *The Use of Technology in the Management of Discovery and the Conduct of Litigation*, 29 January 2009.

[534] Australia, Supreme Court of New South Wales, *Practice Note SC Gen. 7*, 9 July 2008.

[535] In England, the Litigation Support Technology Group has produced a draft exchange protocol for consideration by the Ministry of Justice, and this can be found at the LIST website: <http://www.listgroup.org/the-rules/> at 21 September 2015.

[536] The Canadian Judicial Council has recently published the National Model Practice Direction for the Use of Technology in Civil Litigation, which sets out best practices for exchanging productions in electronic form, as well as handling paperless trials; counsel are encouraged to use a format of exchange which reduces the cost of litigation and improves access to justice; for more information see the Canadian Judicial Council website: <http://www.cjc-ccm.gc.ca> at 21 August 2015.

[537] *Federal Rules of Civil Procedure (2007)* (USA).

[538] For more information, refer to The Sedona Conference website: <http://www.sedonaconference.org> at 21 September 2015.

Guidelines,[539] provides practical advice and practices on how to handle electronic discoveries in order to accommodate the differences that arise between electronic and paper documents.

[5.3.4.3] In Australia, the Federal Court of Australia requires that the party giving discovery must disclose any documents of which they are aware at the time of discovery, after a reasonable search.[540] A list of documents must be provided to the other party and any documents that are no longer in the party's possession, custody or power must be listed separately, along with any privileged documents stating the ground upon which privilege is claimed. In the Federal Court of Australia, *Practice Note CM6*[541] applies to electronic discovery. Discoverable material is exchanged using metadata and images/files for each document.[542]

[5.3.4.4] Federal Court of Australia, *Practice Note CM6* is revolutionary in the sense that it is the first time an Australian court has mandated the use of technology during discovery and at trial, based on a number of assumptions. First, that 'electronic documents, including e-mail, form an increasing proportion of discoverable documents in proceedings before the Court'. Secondly, that 'printing of electronic documents' and 'photocopying paper documents multiple times' is 'a waste of time and cost and rarely necessary'. The Practice Note recognises that there are particular issues borne out of exchanging electronic documents in their native format, so the procedures specified in the practice note are designed to accommodate the unique characteristics of electronic documents in their native format. The Practice Note also provides for de-duplication of electronic documents. Parties are obliged to adhere to the pre-discovery check list where the parties must consider and agree upon the scope of discovery, the strategies for conducting a reasonable search, management of electronic documents, a strategy for the preservation of electronic documents, a timetable and estimated costs for discovery, privileged documents, the document management protocol to be used, the identification of pre-discovery

[539] Ontario Bar Association, Policy & Public Affairs, Ontario E-Discovery Implementation Committee, <http://www.oba.org/Advocacy/E-Discovery> at 17 September 2015.

[540] Australia, Federal Court of Australia, *Federal Court Rules* s 20; any party can service a notice to produce on any other party (s 20.12 and s 20.13). A list of documents is to be produced, as well as an affidavit verifying the list (s 20.16). The list of documents must be given in Form 38.

[541] Australia, Federal Court of Australia, Practice Note CM6 *The Use of Technology in the Management of Discovery and the Conduct of Litigation*, 29 January 2009.

[542] Federal Court of Australia, *Practice Note CM6* provides for a Default Document Management Protocol and an Advanced Document Management Protocol. The Advanced Document Management Protocol is as close to an industry standard protocol as any court protocol has become. Parties should agree to a Document Exchange Protocol (order of court in absence of agreement) and metadata and images/files should be exchange pursuant to the protocol.

conference attendees and any areas of dispute. Focusing parties on these issues follows the way in which courts in the United States of America have addressed the problem of dealing with electronically sourced information (ESI). Hard copy documents and ESI need to be handled very differently and the Federal Court is the first Australian court to recognise this.

[5.3.4.5] In New South Wales, documents can be discovered, pursuant to a notice to produce[543] or an order of the court,[544] if they are relevant to a fact in issue.[545] A list of documents must be provided to the other party and any privileged documents and the reason privilege is claimed, must be stated. *Supreme Court of New South Wales Practice Note SC Gen. 7*[546] sets out the procedure for electronic discovery, and parties can agree to a Document Exchange Protocol or can be ordered by the court to prepare same. Discoverable material is exchanged using metadata and files for each document. Like the Federal Court practice note, the Supreme Court of New South Wales' practice note states that the 'cost of unnecessary photocopying and assembly of documents is unacceptable'. The Practice Note provides that 'discovery of electronically stored documents and information is to be made electronically. Discoverable documents and information that are not stored electronically should only be discovered electronically if it is more cost effective to do so', [547] this was confirmed by Einstein J in *Richard Crookes Constructions Pty Limited v F Hannan (Properties) Pty Limited.*[548] The Practice Note requires the parties to consider preservation of discoverable documents including ESI and to identify any issues with respect to preservation and production.[549] Any difficulties in the recovery of deleted or lost data are to be identified and discussed with the other side.[550] Consideration must be given to the burden and cost involved in discovering documents against the likely importance of those documents,[551] whether particular software is required to access the ESI[552] and to protect the integrity of electronic documents.[553] The parties must meet early in the proceedings to agree upon the format of the electronic databases for e.discovery, the protocol to be used for e.discovery, the type and extent of the ESI to be discovered and whether

[543] Australia, *Uniform Civil Procedure Rules 2005* (NSW) s 21.10.
[544] Ibid s 21.1.
[545] Ibid part 21.
[546] Australia, Supreme Court of New South Wales, *Practice Note SC Gen. 7,* 9 July 2008.
[547] Ibid s 28.
[548] [2009] NSWSC 142 (6 March 2009).
[549] Ibid s 30.2.
[550] Ibid s 30.3.
[551] Ibid s 30.4.1.
[552] Ibid s 30.4.2.
[553] Ibid s 30.4.3.

ESI is to be discovered on an agreed without prejudice basis.[554] The Practice Note provides that the parties need to agree whether the information needs to be reviewed in order to categorise it as privileged or non-privileged and without prejudice to an entitlement to subsequently claim privilege after it has been discovered.[555] The parties must also consider how privileged documents are to be appropriately protected.[556]

[5.3.4.6] In Queensland, a party to a proceeding has a duty to disclose to each other party each document that is in the possession or under the control of the first party and is directly relevant to an allegation in the proceedings.[557] A list of documents must be provided.[558] The Supreme Court of Queensland *Practice Direction 2011/10 - Use of technology for the efficient management of documents in litigation*, outlines the use of information technology in proceedings and Form 19 List of documents provides a sample default protocol for the numbering and objective coding of documents. The Supreme Court of Queensland practice direction encourages the adoption of document protocols from the institution of proceedings and the use of information technology to manage documents for disclosure and for interlocutory and directions hearings and at trial.

[5.3.4.7] In Victoria, a party may serve on any other party a notice requiring discovery for any document in the other party's possession.[559] 'Possession' is defined to include 'possession, custody or power'.[560] (O29 r1). An affidavit of documents[561] listing each document to be discovered and must list any privileged documents, along with the reason for privilege. Supreme Court of Victoria *Practice Note No. 1 of 2007* encourages the use of technology during discovery, however, appears to be primarily concerned with conversion of hard copy documents to an electronic format (images) and capture of objective data about each document. A draft protocol accompanies the practice note which sets out the suggested way in which data is to be captured and exchanged during discovery. However, the practice note makes no provision for native electronic documents.

[554] Australia, Supreme Court of New South Wales, *Practice Note SC Eq 3*, 10 December 2008, s 29.
[555] Ibid.
[556] Australia, Supreme Court of New South Wales, *Practice Note SC Eq 3*, 10 December 2008, s 30.4.5.
[557] Australia, *Uniform Civil Procedure Rules 1999* (Qld) r 211.
[558] Ibid, r 214; the list must be in Form 19.
[559] Australia, Supreme Court of Victoria, *Supreme Court (General Civil Procedure) Rules 2005* (Vic) O29 r2.
[560] Ibid O29 r1.
[561] Ibid Form 29B.

[5.3.4.8] In South Australia, each party must disclose the documents that are, or have been, in the party's possession and are directly relevant to an issue in the pleadings.[562] A list of documents is to be provided,[563] and there is a guideline for the technical format of documents to be provided to the other party.[564] There are provisions for a basic form of electronic disclosure[565] and an advanced form of electronic disclosure,[566] and there are detailed guidelines for advanced electronic disclosure, including de-duplication, formatting, structure and quality of disclosed electronic documents.[567] The parties may apply to the Court for an order that the trial be conducted electronically.[568]

[5.3.4.9] In Western Australia, discovery can be given by notice or order.[569] A list of documents is to be produced,[570] such list to enumerate the documents which are or have been in the 'possession, custody or power' of the party making the list (and separately list those that are no longer in party's possession, custody or power). The list must contain a description of each document and state any privileged documents and the grounds for privilege. While there is no practice note setting out the way in which data is to be prepared for discovery, there are guidelines[571] that can be used as a reference when preparing documents for discovery and if the matter is to be run as an electronic trial.

[5.3.4.10] In Tasmania, the Supreme Court Rules[572] provide that the parties must make mutual discovery of documents that are or have been in their possession, custody or power relating to any matter in question in the action.[573] Rule 384 provides that a list of documents is to be provided by one party to another in Form 26, each document must be enumerated in a convenient order, describe each document or bundle of documents, set out any privileged document and grounds for privilege and be accompanied by an affidavit verifying the list of documents. The Supreme Court of Tasmania is yet to issue a practice note with respect to the

[562] Australia, Supreme Court of South Australia, *Supreme Court Civil Supplementary Rules 2014* (SA) r 138(7).
[563] Ibid r 136(2) in form 29A.
[564] Ibid r 188 and r 135.
[565] *Supreme Court Civil Supplementary Rules 2014* (SA) Chapter 7, Part 3, Division 2.
[566] *Supreme Court Civil Supplementary Rules 2014* (SA) Chapter 7, Part 3, Division 3.
[567] *Supreme Court Civil Supplementary Rules 2014* (SA) rr 119 to 135.
[568] *Supreme Court Civil Supplementary Rules 2014* (SA) r 141.
[569] Australia, Supreme Court of Western Australia, *Rules of the Supreme Court* 1971 (WA) O 26.
[570] Australia, Supreme Court of Western Australia, *Rules of the Supreme Court* 1971 (WA) Form 17 – List of Discoverable Documents, Order 26 r 1(3), r 4(1).
[571] Australia, Supreme Court of Western Australia *Technical Guide for Preparing and Submitting Documents for e-Trials* version 2.03, issued 19 July 2004
[572] Australia, Supreme Court of Tasmania, *Supreme Court Rules 2000* (Tas).
[573] Ibid r 382.

use of information technology in civil litigation and electronic discovery.

[5.3.4.11] In the Northern Territory, discovery is to take place of all documents that are in each party's possession[574] A list of documents is to be prepared[575] identifying the documents, enumerating the documents in a convenient order and contain a description of each document or group of documents, identify those documents no longer in possession of the party and what is believed to have become of them. The *Supreme Court of the Northern Territory Practice Direction No.2 of 2002*[576] *– Guidelines for the Use of Information Technology in Any Civil Matter* is similar to the Supreme Court of Victoria's practice note and the predecessors to the Federal Court and Supreme Court of New South Wales' practice notes.

[5.3.4.12] In the Australian Capital Territory a 'document' has the same meaning as the definition of 'document' in the *Evidence Act 1995* (Cth). The *Court Procedure Rules 2006* (ACT) r 605 provides that a document is discoverable if it relates directly or indirectly to a matter in issue in the proceeding. Disclosure can be by way of notice or order of the court. Each party must file a list of documents in Form 2.23, an affidavit verifying the list and a solicitor's certificate, if the party is represented (r 607). The list must describe each document and set out any documents over which privilege is claimed and the reason for the claim. The Supreme Court of the Australian Capital Territory is yet to issue a practice note with respect to the use of information technology in civil litigation and electronic discovery.

[5.3.4.13] The purpose of the protocols is to provide guidelines for the consistent capture of data, as this in turn leads to efficiency in data exchange and use of data by the parties and the court, and ultimately results in cost savings for the parties.

[5.3.4.14] Protocols should be agreed between the parties before processing of data for discovery commences, as getting changes to the protocol late in proceedings could prove difficult.[577] Every document receives a unique identifier and the premise behind this is that

---

[574] Australia, Supreme Court of the Northern Territory, *Supreme Court Rules 2008* (NT) O 29. 'Possession' is defined in O29 r 1 to include possession, custody or power.

[575] In Form 29A.

[576] Australia, Supreme Court of the Northern Territory, *Practice Direction No.2 of 2002 – Guidelines for the Use of Information Technology in Any Civil Matter*.

[577] See *Jarra Creek Central Packing Shed Pty Ltd v Amcor Limited* [2006] FCA 1802 (24 April 2008 where an initial protocol provided for 14 metadata fields to be discovered and later Jarra sought an additional nine fields. Tamberlin J refused the application on the basis that it would involve substantial additional expenditure of time and cost which Jarra did not offer to meet. Although Jarra contended that Amcor and Visa would have already captured a great deal of the required metadata to assist in their own internal processing of documents, the court

each document should only be numbered once; the importance of this cannot be over-stressed. If documents are numbered more than once, this leads to confusion and inefficiency. For emails, most of the electronic data can be captured automatically, since email contains metadata such as To, From, CC, Date Sent, Subject which can be stripped out programmatically for insertion into a discovery database. However, other electronic files such as MS Office documents and the like, only have limited metadata that can be captured. Information such as To, From and so on has to be manually captured from the face of the document if it is to be absolutely correct. The expense in doing this is not necessary, rather, if native files are exchanged in the way ultimately contemplated by the Federal Court practice note, then users can use their search engines to locate and retrieve relevant documents, which are to be later authenticated.

[5.3.4.15] In summary, the court practice notes in Australian jurisdictions are still designed primarily around hard copy documents. It is timely that courts review such practice notes from the perspective of purely electronic documents, and consider the use of technology to find and retrieve relevant documents, as set out in section 5.4 below.

5.3.5 Discovery & 'Possession'

[5.3.5.1] The court rules provide that documents in the responding party's possession are to be discovered, and many of the court rules state that details of documents that are no longer in the party's possession should be discovered, and these may include documents that have been destroyed. The court rules do not make a distinction between paper and electronic documents, although some of the practice notes and practice directions do refer to the fact that electronic documents are to be discovered, and the format in which they are to be discovery. If documents in a party's possession are to be discovered, then what does that mean, and is 'possession' practically different when referring to electronic documents?

[5.3.5.2] The Macquarie Dictionary[578] defines 'possession' as 'the act or fact of possessing; the state of being possessed; ownership; law actual holding or occupancy, either

noted there was no factual basis for this contention. Tamberlin J agreed that the additional metadata would be useful in conducting searches to reduce the number of discoverable documents, however His Honour did not agree they were necessary in order to justify the additional cost, particularly after the protocol had been agreed a long time previously.

[578] Pan Macmillan Australia, *The Macquarie Dictionary* 2013, 6th edn (1 September 2013), Australia's National Dictionary.

with or without rights of ownership; a thing possessed. The case law looks at 'control'. The term 'control' was considered by the Supreme Court of Queensland in *Equuscorp Pty Ltd v Glengallan Investments Pty Ltd*[579] where Helman J held that control is not necessarily exclusive control, and that the rule will require disclosure of documents even if it is not in the sole possession or control of a party, that is, it is in the party's possession or control jointly with some other person who is not before the court. When offsite records are involved, data may be in a third party's possession and control, such as an Internet Service Provider and such records may need to be subpoenaed. Such subpoena would be directed to the Internet Service Provider.

[5.3.5.3] Interestingly, the question of control over a database came before the English Court of Appeal in *Your Response Limited v Datateam Business Media Limited*[580] (*'Your Response').* In that case, the question before the court was whether the respondent, Your Response, could have a lien over a database for unpaid fees. Your Response posed a number of arguments that it indeed could exercise a lien over the database because (a) it can be considered to be a physical object since it exists in a physical form on servers, (b) the essence of possession is physical control, coupled with an intention to exclude others and that a person can properly be said to possess something if he or she is able to exercise complete control over access to it, (c) a database can be regarded as a document and (d) there is a distinction to be drawn between choses in action and other kinds of intangible property, such as an electronic database. While the court accepted that physical changes are brought about on the storage medium upon which information is stored, the court did not consider that this rendered the information itself a physical object capable of possession independently of the medium in which it is held, and said that the 'distinction is of some importance because of the ease of making and transmitting intangible copies'.[581] Further, the court noted that there is a distinction between a disk or other medium on which data is held (the disk being a tangible object) and the data itself (which is not)[582]. However, with the greatest of respect to the court in that matter, the question is whether, like paper, one can exist without the other? That is, can the data exist without the disk, in the same way that ink on paper cannot exist without its medium?

[5.3.5.4] With respect to the issue of control, the court said that while possession is

[579] [2001] QSC 259 (18 July 2001); note this matter was appealed to the High Court on another point.
[580] [2014] EWCA Civ 281.
[581] Ibid [19] (Moore-Bick LJ).
[582] As recognised in *St Alban's City & District Council, v International Computers Ltd* [1996] 4 All ER 481, which was followed and applied in *Thunder Air Ltd v Hilmarsson* [2008] EWHC 355 (Ch) (unreported).

concerned with the physical control of tangible objects, practical control is a broader concept, capable of extending to intangible assets, which the law would not regard as property at all. While the respondent was entitled to exercise practical control over the information constituting the database, it could not exercise physical control over that information, which was intangible in nature. Whether a database is a 'document', the court discounted this argument, as the basis on which the argument applied, concerned discovery, which was not in issue in this matter. Finally, with respect to whether a database is a form of intangible property different from a chose in action, the court did not accept that argument. Rather, it is intangible property and therefore not subject to a chose in action. In coming to its conclusion, the court analysed the decision in In *OBG Ltd v Alan*[583] where the question was whether intangibles could be the subject of conversion. The majority of the court in that case suggested that the essence of conversion is a wrongful interference with the possession of tangible property, while the minority were of the opinion that intangibles should no longer fall outside the ambit of the law. Ultimately, the court in *Your Response*, concluded that it is a job for Parliament to make such changes to the law in order to legally recognise data as a classification of intangible property.

[5.3.5.5] The courts do tend to distinguish between information on electronic media and the files themselves. Indeed, a digital video recording has been held to be incapable of being 'property'. In *Dixon v R*,[584] the Supreme Court of New Zealand had to determine whether a digital video recording was 'property' within *Crimes Act 1961* (NZ) s 2. That section defines property as including 'real and personal property, and any estate or interest in any real or personal property, money, electricity and any debt, and anything in action, and any other right or interest'.

[5.3.5.6] At first instance, District Court Judge Phillips found that Dixon did obtain property as a result of accessing the computer. However, on appeal, the New Zealand Court of Appeal found, 'after careful consideration',[585] that 'electronic footage stored on a computer is indistinguishable in principle from pure information' and allowed the appeal. The Court of Appeal, said that it is problematic to treat computer data as being analogous to information recorded in physical form. The Court of Appeal found that a computer file is essentially just a

[583] [2008] 1 AC 1.
[584] [2014] NZCA 329 (7 July 2014).
[585] Ibid [31].

stored sequence of bytes that is available to a computer program or operating system, which cannot meaningfully be distinguished from pure information. Ultimately, the Court of Appeal held that the definition of 'property' in the *Crimes Act 1961* (NZ) was not amended to include computer-stored data and therefore, held that the digital video did not fall within that definition; rather the court left it to the Parliament to make such further amendment.[586]

[5.3.5.7] However, the Supreme Court of New Zealand in *Dixon v R*[587] overturned the Court of Appeal decision with respect to whether the digital files were 'property'. The Supreme Court found that 'the digital files at issue are property and not simply information'[588] and considered that 'the digital files can be identified, have a value and are capable of being transferred to others. They also have a physical presence, albeit one that cannot be detected by means of the unaided senses. Whether they are classified as tangible or intangible, the digital files are nevertheless property'[589] for the purposes of the *Crimes Act 1961* (NZ).

[5.3.5.8] The Supreme Court referred to the definition of 'computer system' in the *Crimes Act 1961* (NZ), which the court considered to be a wide definition and includes items such as software and stored data. The Supreme Court concluded that 'there is no doubt that Parliament had stored data in mind when these provisions were drafted. Equally, there is no doubt that Parliament had in mind situations where stored data was copied. "Access" is defined to include receiving data from a computer: data is received from a computer even though it is copied rather than permanently removed from the computer'.[590] The Supreme Court ultimately found that the fundamental characteristic of 'property' is that it is something capable of being owned and transferred.[591]

[5.3.5.9] In *Davies (Daniel) v Police* [592] the New Zealand District Court established that it was not necessary for it to determine whether internet usage was property capable of being stolen because all that was necessary was to establish that internet usage was property for purposes of *Crimes Act 1961* (NZ) s 2 and that elements of offence in s 219 were made out. If internet usage can be considered property, it is indisputable that using the internet is an

[586] Ibid [35].
[587] [2015] NZSC 147.
[588] *Dixon v R* [2015] NZSC 147 at [25].
[589] Ibid.
[590] Ibid at [35].
[591] Ibid at [38].
[592] [2008] 1 NZLR 638.

extension of multiple data files. Furthermore, the Australian case *Australian Property Custodian Holding v Capital Finance*[593] held that a charge can secure an asset that comes into existence after the date of the charge, regardless whether it is tangible or intangible property. Thus, if intangible property such as shares in another company can be the subject of a fixed legal or equitable charge it is possible that data could too be recognised as the subject of a fixed legal or equitable charge.

[5.3.5.10] Whether or not a database can be 'controlled' is an interesting question and in *Your Response*[594] the court concluded that it could not be controlled because it was intangible property, as distinct from tangible property. This position can be juxtaposed with that in intellectual property law, where intangible items are capable of being intellectual property, and are subject to ownership principles such as acquisition, transfer and sale.[595] *Copyright Act 1968* (Cth) s 30 grants the owner exclusive rights and the *Patents Act 1990* (Cth) s 13 grants exclusive rights to the patentee. Both IP and Copyright property can be transferred by the will of the owner, much like selling title to land, or assigned or licensed, much like leasing real property. In Australia, the Supreme Court of New South Wales has ordered that the domain name and associated data be returned to a party in order to prevent further loss or damage; [596] this indicates that data has value in itself in a commercial setting.

[5.3.5.11] In *Dixon v R,*[597] outlined above, the Supreme Court of New Zealand does distinguish *Your Response*.[598] There the Supreme Court found that a digital file can constitute property. This is consistent with the early 20th Century decision in *R v Daye*[599] where the court determined that documents can cover any record of evidence or information and are not limited to tangible documents, illustrating that data, such as a stored system of bytes, is what constructs an electronic document. This is further supported by the Canadian case of *Innovative Health Group Inc. v Calgary Health Region,*[600] which recognises the unique features of electronic

[593] [2012] VSC 124 (4 April 2012).
[594] *Your Response Limited v Datateam Business Media Limited* [2014] EWCA Civ 281.
[595] Refer *Copyright Act 1968* (Cth) which protects ownership of intellectual property. Refer also to the *Personal Property Securities Act 2009* (Cth) ('PPSA'), which came into effect on 30 January 2012 to provide a system registering security interests over both tangible and intangible property. The PPSA includes sub-classes of intangible property, made up of 'account', 'intellectual property', and 'general intangible'.
[596] *Hoath v Connect Internet Services* (2006) 229 ALR 566.
[597] [2015] NZSC 147.
[598] *Your Response Limited v Datateam Business Media Limited* [2014] EWCA Civ 281.
[599] [1908] 2 KB 333.
[600] 2008 ABCA 219 (CanLII).

documents, highlighting the proposition that data is property that can be read and understood on computers. In today's world, it is necessary to appreciate that data is vital and necessary for modern day business operations. In *Your Response,*[601] outlined above, the court posits[602] that if a database of a business is not maintained and improved it will result in being obsolete and useless to the business. Moreover, in the United States of America, damage to a database has been held to be direct physical loss of or damage to property.[603]

[5.3.5.12] In summary, the cases above highlight the inconsistencies in dealing with electronic evidence. The New Zealand cases state a digital file can be 'property', but the English authorities say that a database is an intangible thing and therefore cannot be owned, or possessed. The Canadian authorities recognise that electronic documents have unique features. Under the definition in the *Uniform Evidence Acts*, a database can be included in the definition of a document. However, if the courts are saying that a database is intangible and therefore not considered property, which is inconsistent with the laws of intellectual property and copyright, how does one reconcile ownership or 'possession' of such 'documents' when looking at whether documents ought to be discovered or not and ultimately tendered as evidence? Further, if certain electronic evidence cannot be 'owned', then arguably it cannot be within a person's possession, custody or control and is therefore not discoverable. In terms of admissibility, the electronic 'document' may be admissible, but in order to obtain a copy to admit as evidence, the litigant would need to issue a subpoena to the 'owner' of the document before it can be obtained and tendered in court. This really means that there has to be separate rules about the 'possession' of data that is, who is deemed to be the possessor and what are the attribute of possession. Who would, therefore, be responsible for presenting it to a court upon subpoena?

[5.3.5.13] If electronic information has been held to be incapable of being property, then what of metadata? Ben Grubb, a reporter for the Sydney Morning Herald, recently won the right to have Telstra hand over his metadata relating to his mobile phone. Telstra had initially refused to provide the metadata, on the grounds that he needed a subpoena. However, the Privacy Commissioner found that Telstra has breached National Privacy Principle 6.1 by

[601] [2014] EWCA Civ 281.
[602] Ibid [28].
[603] *NMS Services Inc. v The Hartford*, 62 Fed. Appx. 511, 2003 U.S. App. LEXIS 7442 (4th Cir. Apr. 21, 2003).

failing to provide Mr Grubb with access to his personal information.[604]

[5.3.5.14] Another form of discoverable evidence where 'possession' is questionable, is data under the control of a commercial host, such as social media sites. Is information exchanged on sites such as Facebook is within the 'possession, custody or control' of the user? Even if information on such sites is discoverable, there may be evidentiary issues regarding privacy and authenticity as someone could quite easily create a Facebook profile in someone else's name. Users of social media sites such Twitter, Facebook, IM or MySpace are creating potentially discoverable information and since the information may not be retained on corporate servers, it can complicate electronic discovery. However, this does not mean that the information is inaccessible. It simply means that records may have to be requested from these social networking sites and IM providers as standard discovery procedure (if relevant). While there are no seminal cases in Australian superior courts on the use of social media as evidence, in *Migliore Pty Ltd v Kelly McDonald*,[605] the Full Bench of the Fair Work Commission did look at an employee's Facebook evidence to review an earlier decision regarding whether the employee had been unfairly dismissed. Even in the United States of America, the judiciary has struggled with the logistics of making social media information discoverable, and a number of different methods have been used by the courts. In the United States of America, judges have privately reviewed the information in advance to determine if it should be disclosed,[606] judges have become 'friends' with a party to determine if private Facebook posts were relevant,[607] judges have required parties to turn over physical access, that is, usernames and passwords, for social media accounts to the other party,[608] and a court has fined both a party and his attorney for 'cleaning up' a Facebook page to remove harmful posts and pictures.[609]

[5.3.5.15] In *G & G v Wikimedia Foundation Inc*,[610] a 2009 English case, a businesswoman who had 'confidential and sensitive' details about her professional life as well as her child written onto her Wikipedia page by an anonymous contributor as part of blackmail, won the right to have Wikipedia reveal the IP of the contributor. In the same month, a Maryland appeals court in the US overturned a first-degree felony-murder conviction because one juror

[604] *Ben Grubb and Telstra Corporation Limited* [2015] AICmr [35] (1 May 2015) at [171].
[605] (2013) 236 IR 160.
[606] *Offenback v Bowman Inc*., 2011 WL 2491371 (M.D. Pa. June 22, 2011).
[607] *Barnes v CUS Nashville*, LLC 2010 WL 2265668 (M.D. Tenn. June 3, 2010).
[608] *Largent v Reed* Case No. 2009-1823 (C.P. Franklin Nov. 8, 2011).
[609] *Allied Concrete Co. v Lester*, 736 SE 2d 699 (2013).
[610] [2009] EWHC 3148 (QB).

used Wikipedia to search for some scientific terms relating to how blood flows after death because it denied the accused a fair trial.[611] A defamation case involving Google in the New York State Supreme Court saw the court order that Google provide Liskula Cohen, the plaintiff, with the IP address of an anonymous blogger after Cohen was described as being among 'The skankiest in NYC', as well as being a 'ho'. This has triggered a debate on anonymous Internet speech.[612] Also in the United States of America, emails, electronic journals, diaries and communications were successfully subpoenaed, including entries on websites such as MySpace and Facebook. [613]

[5.3.5.16] Social networking sites can also be used for employee-related claims. For example, to counter allegations of sexual harassment, evidence on a social networking site that a plaintiff routinely invited or encouraged the same type of conversation which they are now complaining of may be relevant. Similarly, photographs posted on a social networking site may be used to show a false claim of compensation for a work-related injury if the photographs show a person dancing at a night club. A further issue that litigants will need to consider when using social media as evidence, as with the use of other content from the Internet is the jurisdiction in which to lodge a claim, given the universality of such material.

5.3.6 Discovery and Documents that have been Destroyed

[5.3.6.1] At common law, any documents that may be required if litigation is 'anticipated', must be retained. What if documents are destroyed? When relevant evidence is lost or destroyed, the court's fact-finding process is compromised.[614]

[5.3.6.2] What if documents have been destroyed? Generally, a party must have a good reason for having destroyed documents that are to be used in evidence, although the definition of what is to be used in evidence is still not clarified at common law. In Victoria, in *British American Tobacco Australia Services Limited v Cowell (as representing the estate of Rolah McCabe, deceased,*[615] the Victorian Court of Appeal reviewed this requirement and said that the test is whether have been destroyed 'in an attempt to pervert the course of justice'.[616] If

[611] Ibid.
[612] *Matter of Cohen v Google, Inc.*, 25 Misc.3d 945, 887 N.Y.S.2d 424 (N.Y. Cty. Aug. 17, 2009) (Madden, J).
[613] Refer *Beye v Horizon Blue Cross Blue Shield* 568 F.Supp 2d 556 (DNJ, August, 2008).
[614] Camille Cameron and Jonathan Liberman, 'Destruction of Documents Before Proceedings Commence: What is a Court to Do?', (2003) 27 *Melbourne University Law Review* 273, 307.
[615] (2002) 7 VR 524.
[616] Ibid.

documents were in a party's possession but are no longer, then the party has an obligation to give a description, date of departing with and belief as to what has become of the document.[617] If there is a belief that documents have been destroyed, then the party is to state when it had been destroyed.[618] The decision of the Victorian Court of Appeal was greatly criticised and the Victorian Attorney-General commissioned a report by Professor Salmon who concluded that 'the broad policy conclusion … is that the exercise of a trial judge's discretion in civil litigation to rule on the consequences of failure by parties to comply with discovery rules should not be limited to circumstances in which formal legal proceedings have been commenced'. This resulted in the enactment of the *Evidence (Document Unavailability) Act 2006* (Vic). That Act deals with document unavailability in a civil proceeding and states that the document is unavailable if it is, or has been but is no longer, in the possession, custody or power of a party to a civil proceeding, and the document has been destroyed, disposed of, lost, concealed, or rendered illegible, undecipherable or incapable of identification, whether before or after the commencement of a proceeding.[619] If in a civil proceeding it appears to the court that a document is unavailable, there is no copy, and the unavailability of the document is likely to cause unfairness to a party in a proceeding, the court may make any ruling or order that it considers necessary to ensure fairness to all parties.[620] The *Crimes (Document Destruction) Act 2006* (Vic) was also enacted to insert new sections into the *Crimes Act 1958* (Vic) to provide sanctions for any person or organisation who destroys documents knowing that the document is reasonably likely to be required in evidence in a legal proceeding.[621] The amendment also provides sanctions were an organisation has a corporate culture which encourages the destruction of documents that are reasonably likely to be required in evidence in a legal proceeding.[622] There are ethical obligations imposed upon solicitors not to destroy documents that are likely to be used in legal proceedings, such as *Legal Profession Regulation 2005* (NSW) r 177. Electronic records may be deliberately destroyed or corrupted. Evidence of how and why records where destroyed will be considered by the court.

[617] *McCabe v British American Tobacco Australia Services Limited* [2002] VSC 73 [182] (Eames J in obiter dictum).
[618] Ibid.
[619] *Evidence (Document Unavailability) Act 2006* (Vic) s 89A.
[620] *Evidence (Document Unavailability) Act 2006* (Vic) s 89B(1).
[621] *Crimes Act 1958* (Vic) s 254.
[622] *Crimes Act 1958* (Vic) s 255.

5.3.7 Discovery & Relevance

[5.3.7.1] If evidence is not relevant, then it will not be admissible. The evidence that is 'relevant in a proceeding is evidence that, if it were accepted, could rationally affect (directly or indirectly) the assessment of the probability of the existence of a fact in issue in the proceeding'.[623]

[5.3.7.2] At common law, the 'train of inquiry' test, as propounded in *Compagnie Financière et Commerciale du Pacifique v Peruvian Guano Co*[624] (Peruvian Guano) case, remains the test of general application for discovery in the High Court. In that case, Brett LJ stated:

> It seems to me that every document relates to the matters in question in the action, which not only would be evidenced upon any issue, but also which, it is reasonable to suppose, contains information which may—not which must—either directly or indirectly enable the party requiring the affidavit either to advance his own case or to damage the case of his adversary. I have put in the words 'either directly or indirectly' because, as it seems to me, a document can properly be said to contain information which may enable the party requiring the affidavit either to advance his own case or to damage the case of his adversary, if it is a document which may fairly lead him to a train of inquiry, which may have either of these two consequences.[625]

[5.3.7.3] However, the test in the Peruvian Guano case has been altered by the various Evidence Acts. As Pincus J explained in *Village/Nine Network Restaurants & Bars Pty Ltd v Mercantile Mutual Custodians Pty Ltd:*[626]

> The law in this State differs from that laid down by Brett LJ in *Compagnie Financiere du Pacifique v Peruvian Guano Co*,[627] in that if a document is not 'directly relevant' to an allegation in issue it need not be disclosed. It is not enough, to justify an order for disclosure, to hold the opinion that 'it is reasonable to suppose [that the document] contains information which may - not which must - either directly or indirectly enable the party requiring the affidavit either to advance his own case or to damage the case of his adversary'. Nor, if a document sought is not directly relevant to an allegation in issue, does it matter whether or not it 'is a document which may fairly lead [the party requiring discovery] to a train of inquiry, which may have either of these two consequences'.[628]

[5.3.7.4] In *Robson v Reb Engineering Pty Ltd*,[629] Demack J stated that 'the word

---

[623] *Evidence Act 1995* (Cth) s 55(1).
[624] (1882) 11 QBD 55, adopted in Australia in *Commonwealth v Northern Land Council* (1993) 176 CLR 604; *Mulley v Manifold* (1959) 103 CLR 341, 345.
[625] *Compagnie Financière et Commerciale du Pacifique v Peruvian Guano Co* (1882) 11 QBD 55, 63.
[626] [2001] 1 Qd R 276.
[627] (1882) 11 QBD 55.
[628] Ibid [7].
[629] [1997] 2 Qd R 102 [105].

"directly" should not be taken to mean that which constitutes direct evidence as distinct from circumstantial evidence. Rather, "directly relevant" means something which tends to prove or disprove the allegation in issue'.[630] The interests of a fair trial require that relevant documents should be discovered by one party.[631] In *Idoport Pty Ltd v National Australia Bank & Ors*[632] the defendant filed a motion seeking discovery of a number of classes of document. Éinstein J held that the 'relevance' test[633] is such that 'a document ... is to be taken to be relevant to a fact in issue if it could or contains material which could rationally affect the assessment of the probability of the existence of that fact (otherwise than by relating solely to the credibility of a witness)… .' The defendants[634] submitted that the documents were relevant as they could all rationally affect the existence or the probability of the existence of that fact.

[5.3.7.5] Being 'relevant' is necessary when undertaking the process of discovery, since any evidence that is not relevant is not admissible. Therefore, it is important to identify any documents that are not relevant early on in the proceedings, so valuable court time is not wasted by endeavouring to admit irrelevant material.

5.3.8 Objections to Discovery

[5.3.8.1] Objections to discovery may be made based on one more reasons such as, the expense and inconvenience likely to be incurred by the respondent in complying, the lack of relevance to the proceedings often referred to as a 'fishing expedition' based on oppression,[635] the lack of particularity with which the documents are described, a claim of privilege, confidentiality, the effect discovery would have on any person and the party was not served with a notice to discover documents. The court, in determining whether documents should be discovered, will consider whether the administration of justice is served by having the document discovery against the reason for the party objecting to the discovery. Where a notice for non-party discovery is served, this too may be objected to on the basis that an unreasonable burden is placed on the respondent, there is a disproportionate expense and effort to the respondent such that it will outweigh the likely benefit to be achieved, the notice is too widely

[630] Ibid.
[631] *NT Power Generation Pty Ltd v Power and Water Authority* [1999] FCA 1623 (9 November 1999).
[632] [2001] NSWSC 435 (22 May 2001).
[633] Australia, Supreme Court of New South Wales, *Supreme Court Rules 1970* (NSW) r.1 part 23.
[634] [2001] NSWSC 435 (22 May 2001) [16].
[635] Refer *Trade Practices Commission v CC (New South Wales) Pty Limited* (1995) 58 FCR 426.

drafted, the notice requires the respondent to form a judgment as to whether the documents are relevant to the issues in the case or it is a fishing expedition. Further, privacy and confidentiality considerations need to be considered and the court will examine the potential effect of the proposed disclosure on those persons.[636]

[5.3.8.2] Until recently, there has been little guidance from the courts on what weight should be given to the factors described above.[637] In the case of *Sony Music Entertainment (Australia) Ltd & Ors v University of Tasmania & Ors*,[638] the applicant sought to obtain certain electronic information so that it could determine the identity and usage history of the respondent universities' computer systems, which the applicants believed had infringed their copyright by illegally downloading and copying music files via the internet. The records sought to be obtained included backup tapes and CD-ROMs. The application was opposed by the respondent universities on the basis that significant quantities of irrelevant documents would be produced and in particular, irrelevant to the identity of certain users. Tamberlin J held that it was within the power of the court to order discovery of a CD-ROM, backup tapes or other electronic stored material, irrespective of whether they contained both relevant and irrelevant information.[639] His Honour considered that the scope of Order 15A conferred a wide discretion upon the court and in this instance ought to be given the fullest possible scope.[640] Tamberlin J was persuaded that some degree of fishing may be appropriate,[641] since neither party was aware of exactly what was contained in the records. His Honour held that appropriate search techniques were to be utilised in the interests of efficiency and restricting access to the respondent universities' data, which would include confidential student data. Wide search techniques were allowed, as His Honour considered that the risk of insufficient discovery was too great if the narrow techniques suggested by the universities were followed.[642] The issues with masking confidential or privileged information, which is often impossible for electronic

[636]Nicolas Suzor, 'Privacy v Intellectual Property litigation: preliminary third party discovery on the Internet' (2004) 25 *Australian Bar Review* 254.
[637] Max Duthie, 'The Subpoena and the Computer: A modern day tale of interrogation and oppression' (2005) *New South Wales Society for Computers and Law*: <https://nswscl.org.au/index.php?option=com_content&view=article&id=120%3Athe-subpoena-and-the-computer-a-modern-day-tale-of-interrogation-and-oppression&catid=27%3Amarch-2004-issue&Itemid=31> at 11 September 2015.
[638] (2003) 198 ALR 367.
[639] Ibid [48]-[54].
[640] Ibid [55].
[641] Ibid [57].
[642] Ibid [62]-[65].

records, could be overcome by imposing undertakings in relation to non-disclosure and confidentiality upon the retriever.

[5.3.8.3] If there are objections to documents being discovered, then there will certainly be objections to the evidence if it is sought to be tendered as evidence. Interlocutory proceedings to determine relevance early in the proceedings can save court time later. Arguments as to 'fishing' may be considered when looking at whether hard drives, and the information contained upon the hard drives, can be discovered, and this is examined further in sections 4.3.2 and 4.3.8.

5.4 Processing, Reviewing & Analysing Electronic Evidence

[5.4.1.1] Locating relevant documents to use as evidence in any proceeding, is the key to ensuring relevant, authentic evidence is presented to the court. When dealing with electronic documents, volumes are typically much larger compared with hard copy documents, for example, one gigabyte of data can contain up to 250,000 pages of material. The ability to search through electronic documents means that locating relevant documents is easier, as target searches can be conducted without the need to have a team of paralegals look at every document. Some cases, particularly in the United States of America, have indicated that lawyers must be using the latest search techniques to locate relevant documents.[643] When culling and filtering documents for discovery, the metadata can be critical, especially timestamps, in order to determine if files are authentic. Culling and filtering techniques, examination of metadata, and search technologies are examined below.

5.4.2 Culling and Filtering

[5.4.2.1] As with paper document discovery, only a small number of electronic documents may be required to be discovered and these have to be identified and set apart from the others. The first step in any electronic discovery, is to cull and filter as many irrelevant documents as possible. Certain file types can immediately be removed from a data set, because they are irrelevant.[644] For example, files which run operating systems, such as Microsoft Windows or applications such as Microsoft Office applications, can be identified and removed

[643] *Da Silva Moore v Publicis Groupe*, 11-civ-1279 (ALC) (AJP), U.S. Dist. LEXIS 23350 (S.D.N.Y. Feb. 24, 2012).
[644] Eoghan Casey, ed, *Handbook of Computer Crime Investgation: Forensic Tools and Technology* (Academic Press, United Kingdom, 2002), 45.

from the repository.[645] These types of files would not exist in paper repositories. Simple filters include identifying key custodians in the matter and focusing on the location of their documents, identifying the relevant date periods and filtering out documents which fall outside this range and identifying exact duplicates. More complex filters include identifying near duplicates, conducting keyword searches and utilising Technology Assisted Review. Preserving file metadata and timestamps throughout electronic document productions is essential for authentication of electronic documents.

[5.4.2.2] Date and time information within the metadata of files can be extremely useful in evidence. Virtually all electronic documents contain metadata embedded within the electronic document, which contain certain dates, which computer forensic programs can extract and search. There can be a number of different date and timestamps on electronic documents. For example, each Microsoft Office file has two sets of relevant dates. First, there are file system dates, often referred to as 'timestamps', which are independent of Microsoft Office metadata.[646] When electronic files are copied from one computer to another, metadata is often altered. Secondly, there are Microsoft Office dates which are contained within the MS Office file itself and which are created and altered when using Microsoft Office. Microsoft Word, stores various dates in the metadata, such as the Date Created, which is the date the document was created (although this can be misleading where a document is copied and used as if it were an original), the Date Last Modified, which is the date the document was last modified) and the Date Accessed, which is the date the document was last accessed, without modification. Unlike the Date Created field, the Date Last Modified field is not altered when a file is moved from one computer to another. It changes only when the contents of the file have been changed and saved in some way. However, the Date Last Modified field is a more recent introduction to the Microsoft package so it may not be found for files from older

[645] Service providers often keep a library of MD5s of known operating system and application specific files, so that once each file has its own MD5 generated, it can be compared against the library and removed if matched. Whilst the technical process is important the supervision of the process and the guarantee of integrity of the operation is critical to legal efficacy. Certain file types may be excluded based on specific knowledge of the matter. For example, it may be known that CAD drawings (AutoCAD DXF (Drawing Interchange Format, or Drawing Exchange Format)) will not be required for discovery, so all CAD drawing files can be excluded from the pool of potentially discoverable documents. Filtering needs to be done based on a file header analysis of the documents, rather than simply relying on file extensions. This is because file extensions can be easily changed, particularly if a user wants to hide certain documents. A file header analysis involves a software application which analyses the document as a whole to determine if all the elements of the document match the file extension (this is explained further in section 5.6.1).

[646] These are stored in the FAT (File Allocation Table) or the NT File System (NTFS) which is like to a table of contents for the operating system (for example, Microsoft Windows).

versions. The Date Created field may be retained within MS Office metadata properties, but change within the operating system file system properties. The Date Accessed field is the date the file was last accessed. In this situation, 'access' is interpreted very loosely. In addition to opening a file and saving it without changes, copying a file from one computer to another also changes the Date Accessed field on the first computer. The Date Accessed field is also changed if the file properties are inspected, even if the file was not opened. When using functions such as 'Save As', some metadata from the existing file will be saved, for example Date Printed will be kept. [647]

[5.4.2.3] All metadata and timestamps can be altered, and this can affect authenticity of electronic documents. There are free utilities that can be easily downloaded which alter the 'Date Created' and other metadata fields. An easy way of knowing if metadata was altered is if there is a conflict between metadata and timestamps within a file and surrounding files. Analysis of other areas of the computer that could support or deny a claim is often required.[648] A user can attempt to change the metadata in a file by changing the computer's system clock. If this is suspected, a computer forensics expert can the Date Accessed fields, and also examine files created using internet timestamps, such as cookies,[649] internet cached files or email.[650] These files obtain their timestamp from the internet server which created the file, so can be compared with other timestamps on the computer to determine if the times reconcile. The expert can also search for 'link files' which are essentially shortcuts created each time a file is created. These are located in the file system and in the registry. There is a reference to each 'link file' in 'Recent Documents' in the computer's registry. If a document has been opened, forensic software tools can be used to examine all Last Accessed dates and determine what was opened, when it was opened and whether it was copied. The physical identification number may also be discovered.

---

[647] See further Michael C. Weil, 'Dynamic Time & Date Stamp Analysis' (2002) 1(2) *International Journal of Digital Evidence*, <http://www.utica.edu/academic/institutes/ecii/publications/articles/A048B1E4-B921-1DA3-EB227EE7F61F2053.pdf> at 11 September 2015, where various key dates and times are listed such as MAC Time, System Time, Approximate Actual System Time, Actual Time, Dynamic Date and Time Stamp, Dynamic Date and Time Stamp Analysis and Date and Time Standardisation.

[648] For example, in Microsoft Windows, the index.dat files contain records of when the user opens a document. Recovering and analysing the file access activity in the index.dat can help support claims that suggest the file was created or revised at a specific time or date.

[649] A cookie is a small file which stores information related to a user's internet activity and provides reports back to the website that created the cookie.

[650] If a user changes the clock on a computer, then this change will be stored in the 'timedate.cpl' file on the hard drive.

[5.4.2.4] Data can be filtered by only reviewing those documents relevant to particular persons. With email, identifying custodians can be relatively easy, since each user will most likely have an email file identified by their name (assuming the person is correctly identified). Email repositories relevant to that particular custodian can be collected and processed for review. Electronic files relevant to custodians may be a little more difficult to identify, since users may create and save electronic files in a number of disparate locations (the various locations in which data may be stored is explored more fully in section 5.2). By way of example, if the legal team agrees that only emails and electronic documents created by, and received by, say six people within the organisation, the email repositories for those six people only will need to be forensically copied. In addition, the home directories for each custodian are forensically copied for review, as well as files from each person's notebook computer, since each person regularly takes their notebook computer home and saves files to the notebook's hard drive.

[5.4.2.5] The culling and filtering process, undertaken by electronic evidence specialists, must be undertaken in such a way that preserves the integrity of the files. If lawyers tamper with original evidence, this may alter the metadata and thereby compromise the integrity of the system such that the other party to the matter can legitimately claim that the presumption contained within *Uniform Evidence Acts* ss 146 and 147 can be rebutted. It is the responsibility of the lawyers producing the material to prove the integrity of evidence, if it is called into question by the other party.

5.4.3 De-duplication & Near De-duplication

[5.4.3.1] De-duplication is the identification of identical copies of electronic documents. De-duplication is carried out using a method which allows each file to be given a unique 'digital fingerprint'. Each file is given an MD5 hash algorithm[651] or an SHA-1 hash algorithm.[652] This de-duplication method represents a pure technical comparison of data. Each file with the same hash algorithm will be marked as duplicates. When processing large repositories which are

[651] MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5 is currently a standard, Internet Engineering Task Force (IETF) website: <http://www.ietf.org> at 11 September 2015. The IETF is the body that defines standard Internet operating protocols such as TCP/IP.

[652] SHA-1 is the US Secure Hash Algorithm takes a message of less than 264 bits in length and produces a 160-bit message digest designed so that it is computationally very expensive to find a text string that matches a given hash.

received in tranches, new files added to the discovery can be de-duplicated by comparing hash algorithms. Emails are de-duplicated in a different way to other electronic files, since emails with different hash algorithms may still be duplicates for review purposes. The way in which emails are de-duplicated is best explained by way of example. If John Smith sends an email to Samantha Jones, and cc's Tom White, Aladdin Cave and Tim Stone. When reviewing that email in John Smith's Sent Items and Samantha Jones', Tom White's and Aladdin Cave's Inboxes, it is important to identify each of these as duplicates so each copy is not reviewed several times. Certain metadata fields are compared to confirm that the email is indeed a duplicate.

[5.4.3.2] Near de-duplication allows documents that are similar but not identical to be grouped together. This technology is explained further below in section 5.4.5.

[5.4.3.3] Identifying exact duplicates assists in reducing the volume of documents in any discovery, however, it is should be remembered that with electronic documents, identifying an original document can be difficult, if not impossible.[653] However, if required to authenticate an electronic document, it may be necessary to show other iterations of that document, in order to determine provenance. Proving exact duplicates is a technical issue, which can be demonstrated by the use of software that compares the 'digital fingerprint' of one document to another.

5.4.4 Keyword Searching

[5.4.4.1] When document sets were paper based, legal review was performed in a linear manner, that is, the reviewers would start at the first document and review each separately until they reached the end. When paper documents were imaged, data about each document would be captured that allowed the reviewers to at least sort documents by date and author to assist in streamlining the review. Later, technology became available which allowed imaged documents to be converted to text so that searches could be conducted across the documents themselves. However, imaging a hard copy and converting it to text does not render the text exactly, so some words could be missed. The benefit of searching across electronic documents is that every word in every document is already in electronic format and is not subject to the vagaries of poor quality images. Further, the traditional linear review is no longer practicable with the

[653] Refer Paul, above n 25 and Mason, above n 178 [10.32].

volume of electronic documents to review. Consequently, keyword searching became popular and is now commonplace in culling documents for electronic discovery review.

[5.4.4.2] Simple keyword searching alone can be inadequate. This is because simple keyword searches are both over- and under-inclusive, given the nuances in the language. Traditional keyword searches identify all documents containing a specified term, but do so in a way which may be out of context.[654] Further, basic keyword searches can miss documents that may be relevant.[655] Some search terms could have different meanings, depending on context and a responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.[656]

[5.4.4.3] Studies on the effectiveness of keyword searching date back 30 years. A 1985 study by Blair & Maron[657] on a rail accident in San Francisco asked an experienced legal team to develop keyword searches to identify the relevant documents out of a set of 40,000 documents. They were allowed to keep refining their keyword set until they felt comfortable they had found a high percentage of relevant documents, at least 75%. The results of those keyword searches were then analysed against the true relevance of every document in the 40,000 to see if their keyword search was actually effective. What the study found was that the keyword search had only achieved a shockingly low 20% recall, meaning 80% of the relevant documents in the case would have been missed using keywords and never reviewed at all. Other studies have shown higher levels of recall are possible using keywords, but can be difficult to achieve.

[5.4.4.4] In 2006, an independent research project was designed to compare the efficacy of various search methods. The Text Retrieval Conference (TREC) was interested in ascertaining whether alternative search technologies performed better than Boolean

[654] Jason R Baron ed., 'The Sedona Conference Best Practices and Commentary on the Use of Search and Information Retrieval Methods in E-Discovery' (August 2007) 8 *The Sedona Conference Journal* 189 at 201 where the Sedona Conference uses the example of the term 'strike' which can be found in 'documents relating to a labor union tactic, a military action, options trading, or baseball, to name just a few (illustrating 'polysemy', or ambiguity in the use of language)'.

[655] Ibid where The Sedona Conference gives the example of an email 'referring to a 'boycott' if that particular word was not included as a keyword, and a lawyer investigating tax fraud via options trading might miss an email referring to 'exercise price' if that term was not specifically searched'.

[656] *Air Canada v Westjet Airlines Ltd* (2006) 267 D.L.R.(4th) 483 (Ont. Sup. Ct) [20]. In that case, the court stated that it would not consider a process that relied almost entirely on electronic searches.

[657] David C. Blair and M. E. Maron, 'An Evaluation of Retrieval Effectiveness for a Full-Text Document-Retrieval System' (1985) 28(3) *Communications of the ACM*, 289-299.

searches.[658] TREC used a test set of 7 million documents that had been made available to the public pursuant to a Master Settlement Agreement between tobacco companies and several state attorneys general. Sample document requests (topics) were prepared. The topic creator and a TREC coordinator then took on the roles of requesting and responding lawyers to work out a form of Boolean search to be run for each document request. In addition, 31 different automated search methodologies, including concept searching, were used to locate documents relevant to the topics. On average, across all of the topics, the Boolean searches located 57% of the known relevant documents.[659] None of the alternative search methodologies reliably performed any better. Interestingly, the alternative search methodologies did not necessarily retrieve the same responsive documents. When the responsive documents found by the alternative search technologies were combined, there were an additional 32% documents in each topic. Although the Boolean searches performed better on individual topics against individual search alternatives, the combined result meant that some responsive documents were found that the Boolean searches missed. This could perhaps mean that Boolean searches, if used in conjunction with other alternative search methods will have greater potential in locating all potentially relevant documents. Baron, Lewis and Oard concluded that Boolean searches remained the state-of-the art and most appropriate search technology, especially when keyword or Boolean searches are used in an iterative manner where litigants (a) negotiate search terms and Boolean operators, (b) run the agreed-upon searches, (c) review the preliminary results and (d) adjust the searches through a series of meet-and-confers.[660] As part of its study, TREC employed an expert tobacco document searcher who used an 'interactive' search methodology. TREC found that the expert searcher located, on average, an additional 11% of the relevant documents beyond those that had been located by the initial Boolean searches. This suggests that an interactive Boolean approach located 68% of the relevant documents, a higher percentage than any of the alternative search methodologies.

[5.4.4.5] In 2007, the Sedona Conference issued *The Sedona Conference® Best Practices Commentary on Search & Retrieval Methods (August, 2007),*[661] which set out best practice for key word searches. The Sedona Conference suggested several best practice points on how

[658] Jason R. Baron, David D. Lewis & Douglas W. Oard, *TREC-2006 Legal Track Overview* (2006) Text REtrieval Conference <http://ece.umd.edu/~oard/pdf/trecov06.pdf> accessed at 21 November 2014.
[659] Ibid.
[660] Ibid.
[661] Jason R Baron ed., 'The Sedona Conference Best Practices and Commentary on the Use of Search and Information Retrieval Methods in E-Discovery' (August 2007) 8 *The Sedona Conference Journal* 189.

parties should structure any search and retrieval methods.[662] The choice of a specific search and retrieval method will be highly dependent on the specific legal context in which it is to be employed. Further, the Sedona Conference considered that the use of search information retrieval tools does not guarantee that all responsive documents will be identified in large data collections, due to characteristics of human language. Moreover, differing search methods may produce differing results, subject to a measure of statistical variation inherent in the science of information retrieval. The Sedona Conference considered that the parties should make a good faith attempt to collaborate on the use of particular search and information retrieval methods, tools and protocols (including keywords, concepts and other types of search parameters). Finally, the Sedona Conference stated that the parties should expect that their choice of search methodology will need to be explained, either formally or informally in subsequent legal contexts (including in depositions, evidentiary proceedings and trials).[663]

[5.4.4.6] In 2008, Judge Grimm in the United States District Court for the District of Maryland, delivered a seminal judgment on the issue of the use of keyword searches to locate relevant documents during discovery. In *Victor Stanley v Creative Pipe, Inc.,*[664]*('Victor Stanley'),* a joint protocol contained detailed search and information retrieval instructions, including nearly five pages of keyword/phrase search terms to assist in locating relevant documents. The joint protocol contained detailed search and information retrieval instructions, including nearly five pages of keyword/phrase search terms. The defendant also used keywords to locate privileged documents, but when the discovery was exchanged, the other party found privileged documents and then notified the defendant accordingly. The defendant claimed the privileged documents had been provided inadvertently. Upon reviewing the keyword lists, the court was scathing of the process used. The court stated that the defendants were 'vague in their description of the seventy keywords used', how they were developed, how the search was conducted and what quality controls were employed to assess their reliability

[662] Redgrave, J.M *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery*. (Ed), , 2nd ed, (2007) The Sedona Conference, Sedona.

[663] Ibid.

[664] 250 F.R.D. 251 (D. Md. 2008). This case considered two earlier cases, *United States v O'Keefe,* 537 F. Supp. 2d 14, 24 (D.D.C. 2008) and *Equity Analytics, LLC v. Lundin* 248 F.R.D. 331, 333 (D.D.C. 2008). Those cases required that the parties be prepared to support their positions with respect to a dispute involving the appropriateness of ESI search and information retrieval methodology (an area of science and technology) with reliable information from a qualified person who can provide helpful opinions as opposed to counsel providing conclusory arguments.

and accuracy.[665] Judge Grimm went on to say that 'while it is universally acknowledged that keyword searches are useful tools for the search and retrieval of ESI, all keyword searches are not created equal; and there is a growing body of literature that highlights the risks associated with conducting an unreliable or inadequate keyword search or relying exclusively on such searches for privilege review.'[666] His Honour said that common sense suggests that even a properly designed and executed keyword search may prove to be over-inclusive or under-inclusive, resulting in the identification of documents as privileged which are not, and non-privileged which, in fact, are. The only prudent way to test the reliability of the keyword search is to perform some appropriate sampling of the documents determined to be privileged and those determined not to be in order to arrive at a comfort level that the categories are neither over-inclusive nor under-inclusive. There is no evidence on the record that the defendants did so in this case.'[667] Leaving aside the issues of waiver of privilege, Judge Grimm did conclude that the defendants neither identified the keywords selected nor the qualifications of the persons who selected them to design a proper search. Further, the defendants had failed to demonstrate that there was quality-assurance testing and that when their production was challenged by the plaintiff, and had failed to carry their burden of explaining what they had done and why it was sufficient. Finally, and in any event the court held that the defendants had waived protection of privilege. Selection of the appropriate search and information retrieval technique requires careful advance planning by persons qualified to design effective search methodology. When selecting a methodology to be implemented, the methodology selected should be tested for quality assurance, the party selecting the methodology must be prepared to explain the rationale for the method chosen to the court, demonstrate that it is appropriate for the task, and show that it was properly implemented and there should be compliance with the Sedona Conference Best Practices.

[5.4.4.7] The message to be taken from *Victor Stanley*, is that when parties decide to use a particular ESI search and retrieval methodology, they need to be aware of literature describing the strengths and weaknesses of various methodologies,[668] and select the one that they believe

[665] Ibid.
[666] Ibid.
[667] Ibid.
[668] For example, Jason R Baron ed., 'The Sedona Conference Best Practices and Commentary on the Use of Search and Information Retrieval Methods in E-Discovery' (August 2007) 8 *The Sedona Conference Journal* 189; Maura R. Grossman & Gordon V. Cormack, 'Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review' (2011) 17(3) *Richmond Journal of Law and Technology* 1, 37; Gordon V. Cormack and Maura R. Grossman, Evaluation of Machine-Learning Protocols for

is most appropriate for its intended task. Should their selection be challenged by their adversary, and the court be called upon to make a ruling, then they should expect to support their position with affidavits or other equivalent information from persons with the requisite qualifications and experience, based on sufficient facts or data using reliable principles or methodologies.

[5.4.4.8] Alternative search technologies are being investigated by litigants and their lawyers to assist with search strategies, and such alternatives include 'concept searching'. There are three principal search techniques referred to as 'concept searching',[669] clustering, taxonomies and ontologies and Bayesian Classifiers. Taxonomy tools are used to categorise documents containing words that are subsets of the topics being searched for. For example, if the concept 'cats' is being searched for, then the taxonomy tool would also locate documents that mention 'Russian blue' and 'Persian'. Ontology tools are not confined to subsets but would instead also locate documents that mention 'veterinarians'. Bayesian Classifiers are systems that use probability theory to make educated inferences about the relevance of documents based on the system's prior experience in identifying relevant documents. Search results are ranked based on the predicted likelihood of relevance.

[5.4.4.9] In 2009, Judge Andrew Peck in the New York District Court took the bold step of instructing the Bar that a 'wake-up' call was needed for 'careful thought, quality control, testing and cooperation with opposing counsel in designing search terms or "keywords" to be used to produce email or other electronically stored information'.[670] Any proposed methodology for key words should be quality control tested to assure accuracy in retrieval and elimination of 'false positives'.[671] This leads to a discussion of more advanced forms of searching, known as Technology Assisted Review.

Technology-Assisted Review in Electronic Discovery, at: <http://www.wlrk.com/webdocs/wlrknew/AttorneyPubs/WLRK.23339.14.pdf> at 11 September 2015.

669 Christopher H. Boehning, and Daniel J. Toal., 'In Search of Better E-Discovery Methods' *New York Law Journal* (online) 23 April 2008.

670 *William A. Gross Construction Associates, Inc. v. American Manufacturers Mutual Insurance Co.*, 256 F.R.D. 134, 136 (S.D.N.Y. 2009) (Peck, M.J.); see also Hon. Andrew Peck, 'Search, Forward - Will manual document review and keyword searches be replaced by computer-assisted coding?' Law Technology News (online), 1 October 2011 <http://www.lawtechnologynews.com/id=1202516530534/Search-Forward> at 11 September 2015.

671 Ibid.

5.4.5 Technology Assisted Review

[5.4.5.1] Technology Assisted Review is being lauded as a way to locate relevant documents for discovery, and of course it is only relevant documents that can be admitted as evidence. Technology Assisted Review helps lawyers find relevant documents in a much more efficient and cost effective manner compared to traditional linear review which often meant relying on junior lawyers who may not have fully understood the case, and who were faced with a long and tedious process of reviewing hundreds of documents during an eight (or more) hour shift. Technology on the other hand, is not subject to fatigue, hangovers, gossip or being ill-informed. These tools use every word in every document to assign relevance as determined by the senior lawyer on the matter. Technology Assisted Review can include a number of different 'clever' technologies, and is an area in which research is ongoing in order to find even more clever ways of finding what lawyers seek in a repository of documents. These technologies include 'clustering', 'concept searching', 'email threading', 'near de-duplication' and 'predictive coding'. In-built features, such as predictive coding are being celebrated as the answer to help curtail ever-increasing litigation costs for both in-house and external counsel.

[5.4.5.2] Clustering technology can be used to group together emails and other electronic documents that relate to the same topic. Clustering relies on statistical relationships which result in documents with similar words being clustered together. The clustering software compares each document in a set to a 'pivot' document which has already identified as relevant. The more words a document has in common with the pivot document, the more likely it is to be about the same topic and therefore relevant. The clustering software ranks documents based on their statistical similarity to the pivot document. Clustering can be used as a helpful tool for initial categorisation. The algorithms in the software analyse the actual content of individual documents- allowing them to be sorted into related 'clusters' or groups. The solution scans the content of each document and, by cross-referencing against a specialised index, identifies recurring key concepts. Documents dealing with discrete concepts can then be batched to individual reviewers, again so documents of a similar concept can be reviewed together.[672]

[5.4.5.3] Concept searching allows the technology to determine relevance by associating words with particular concepts. For example, if the term 'Java' is being searched, then the

[672] John Jay College of Criminal Justice, Towards Scalable E-discovery Using Content-based Hierarchical File Clustering (John Jay College of Criminal Justice, 2013), 23.

concept search engine would be able to identify whether it is 'Java' the Indonesian island, 'Java' the scripting language or 'Java' coffee beans are more relevant to the user. The concept search engine will still locate the other concepts, but will order them lower in relevance ranking than the relevant concepts. When using a tool such as 'concept searching' a reviewer's workflow can be set so that the reviewer can review documents that may be associated with a particular issue or concept, so that they are reviewing documents that are similar in nature. In a traditional linear review, two different reviewers may review documents that are of similar concept, but this correlation may be missed because the two documents are reviewed in context with each other. By utilising the power of the technology, the efficiency of the review increases enormously. Each reviewer would then see *all* of the documents related to a particular concept and this approach gives the reviewer additional context and enables him or her to quickly move through each conceptual batch, coding with more accuracy and consistency. By the time he or she finishes a particular batch, a reviewer should be an 'expert' on whatever concept was grouped into that batch. Through conceptual batching there are advantages to be made where teams can structure the review to better meet the team's priorities. While the conceptual groups are generally software-created, once generated, a quick check of each cluster allows the case team to select those that are most relevant or most interesting for priority review. Likewise, conceptual clusters that are clearly irrelevant can be de-prioritised or bulk-tagged as such.[673]

[5.4.5.4] 'Email Threading'[674] is another example of where technology assisted review really increases productivity. Email Threading allows the reviewer to simply review the email that is last in the email thread; that email will include the whole conversation and the reviewer can determine if the whole thread is relevant or not. Therefore, instead of reviewing a number of related documents, or again seeing the documents out of context with one another, one document is reviewed to determine the relevance of many documents that are related. In a traditional review, no single reviewer is likely to see the entire thread and therefore misses out on the whole conversation.

[5.4.5.5] Near de-duplication allows documents that are similar, but not identical, to be identified and grouped together, based on a certain percentage similarly, which is set by the

[673] See further: EDRM Website on Search Methodologies: <http://www.edrm.net/resources/guides/edrm-search-guide/search-methodologies> at 12 January 2015.

[674] See further: EDRM Website definition of email threading: http://www.edrm.net/resources/glossaries/grossman-cormack/email-threading at 12 January 2015.

user when conducting the near de-duplicate search.[675] A pivot document is selected against which similar documents are compared, and then highlighted to the user. Differences between each similar document as compared to the pivot document are marked up so that the user can review these to determine if such documents are indeed duplicates for the purposes of the review, or for example, a different version of the pivot document. The differences are highlighted in much the same way that differences are highlighted using the 'compare' function in MS Word.

[5.4.5.6] Predictive coding is a method where the user can 'train' the system to recognise documents that are relevant. A senior lawyer will be presented with a random set of, say, 500 documents from the repository which the lawyer will then mark as 'relevant' or 'not relevant'. The technology will then determine, from the words in each of the relevant documents, what other documents are relevant. The lawyer can review further randomly presented sets of documents, until the system learns what is relevant. There are two primary terms in predictive coding; precision and recall. Precision is the percentage of documents that lawyers review that are actually relevant. It is a measure of how efficient the reviewers are, and how much time is wasted reviewing non-relevant documents. The higher the precision rate percentage, arguably the more efficient and cost effective the review. Recall is an illustration of how many documents are being missed and are not reviewed at all. In a perfect world with a reviewer who never makes a mistake, he or she would review every document in the document repository and would have 100% recall. The lower the recall rate the more relevant documents are missing.

[5.4.5.7] To compare the effectiveness of predictive coding with other review methods such as traditional linear (or manual) review or keyword searching or predictive coding, the results can be measured by the levels of precision and recall. Judge Cote in the New York District Court has confirmed that 'predictive coding had a better track record in the production of responsive documents than human review'; *Federal Housing Finance Agency v HSBC North America Holdings Inc, et al.*[676] Her Honour went on to say that although both predictive coding and human review fell short of identifying for production all of the documents the parties in

[675] See further: EDRM Website definition of near duplicate detection: http://www.edrm.net/resources/glossaries/grossman-cormack/near-duplicate-detection at 12 January 2015.
[676] 2014 WL 584300, 3.

litigation might wish to see, 'no one should expect perfection for this process'[677]. Her Honour made the point that parties in litigation are required to act in good faith during discovery and that production of documents can be a herculean undertaking often requiring clients to pay vast sums of money. All that can be expected, said her Honour, was that 'good faith, diligent commitment to produce all responsive documents uncovered when following the protocols to which the parties have agreed, or which a court has ordered'. The point of this case is to highlight that the use of technology such as predictive coding is becoming an accepted method of review during discovery and that indeed, can be more accurate than human review. The court made reference to an article published by Grossman and Cormack in *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review,*[678] where the authors compared the results of a review by humans against a review done using predictive coding; the results showed that predictive coding was more accurate and efficient.

[5.4.5.8] Although Australian courts have yet to decide whether technology such as predictive coding is an accepted method of review, many law firms are using this technology to assist in review of electronic documents for discovery. In the United States of America, in the case of *Da Silva Moore v Publicis Groupe,*[679] Magistrate Andrew J Peck, issued the first decision in a court in the United States of America, specifically addressing the use of predictive coding as a replacement for traditional linear document review. During argument, the plaintiffs expressed concerns about the accuracy of the original coding and the possibility that the software would overlook relevant documents. Judge Peck stated that while many lawyers have embraced the technology, several are reluctant to because of the risk of legal sanction. With the order, Judge Peck has now removed that risk. As the court noted, 'statistics clearly show that computerized searches are at least as accurate, if not more so, than manual review.'[680] Citing a recent study, Judge Peck claimed that technology-assisted review is more accurate and fifty times more economical than exhaustive manual review. The ruling concluded with Judge Peck reasoning that 'the use of predictive coding was appropriate considering…the superiority of computer-assisted review to the available alternatives (i.e., linear manual review or keyword

[677] Ibid.
[678] Maura R. Grossman & Gordon V. Cormack, 'Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review' (2011) 17(3) *Richmond Journal of Law and Technology* 1, 37.
[679] 11-civ-1279 (ALC) (AJP), U.S. Dist. LEXIS 23350 (S.D.N.Y. Feb. 24, 2012).
[680] Ibid 28-29.

searches)'.[681]

[5.4.5.9] Judge Peck's decision exemplifies the changing nature of discovery for lawyers. In his ruling, Judge Peck stated his long held position the legal industry needs to embrace predicative coding and other technological processes as they continue to play an increasingly useful and relevant role in the justice system. Addressing lawyers, Judge Peck stated:

> What the bar should take away from this opinion is that computer-assisted review is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review.

[5.4.5.10] In the subsequent case of *Rio Tinto PLC v. Vale S.A.*,[682] Judge Peck, after providing a brief history of cases where courts have allowed technology assisted review (TAR) where the parties agreed, Judge Peck stated that 'it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it'.[683] Judge Peck noted that though the extent to which adverse parties must cooperate in sharing TAR training documents is unsettled, the parties may choose to cooperate, as they did in this case, and should be encouraged to do so. Finally, Judge Peck stressed that 'it is inappropriate to hold TAR to a higher standard than keywords or manual review. Doing so discourages parties from using TAR for fear of spending more in motion practice than the savings from using TAR for review'.[684]

[5.4.5.11] With predictive coding, instead of using keywords to find documents, entire documents are indexed and the system is 'taught' which documents are relevant and which are not relevant, by having a lawyer review a random set of documents, and the system then uses algorithms to 'learn' what is relevant from the relevant documents selected. The system then finds documents that are conceptually similar to the relevant documents. Through rounds of teaching the system, say 1,000 documents at a time, the system is able to keep increasing the recall percentage until the high standard established by Judge Peck is achieved. Although the algorithms are advanced and not transparent to a lay user, the concept is not totally foreign, as anyone using a Google search has experienced advanced algorithms finding the webpages they

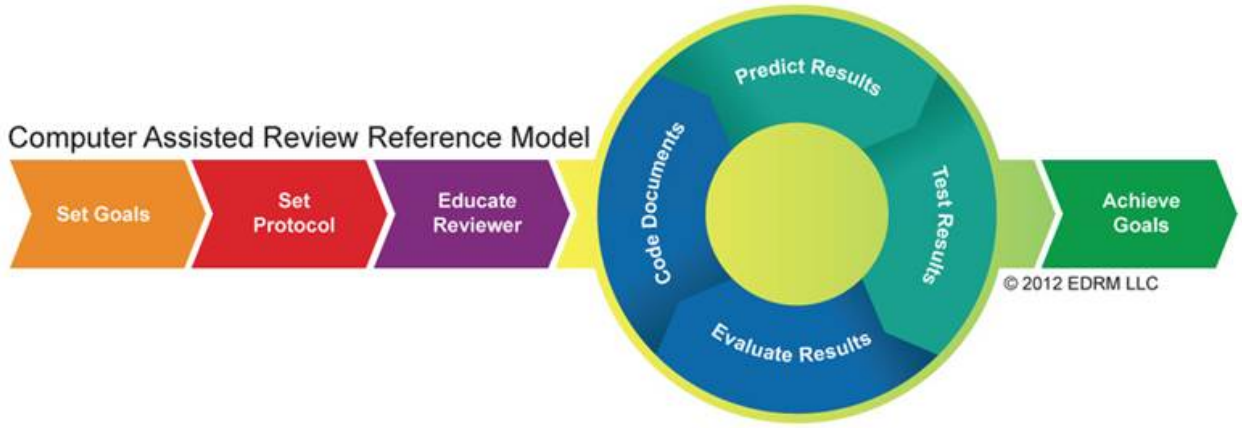
[681] Ibid.
[682] 2015 WL 872294 (S.D.N.Y. Mar. 2, 2015).
[683] Ibid at 2.
[684] Ibid at 3.

intend (not simply which words appear in the websites).

[5.4.5.12] In a typical review undertaken by paralegals, a document set of 35,000 documents might achieve a recall rate of about 50%, in other words, half of the relevant documents may be missed. By contrast, if a senior associate reviews 4,500 utilising the random review process set out above, she might also achieve a recall rate of 50%. However, if the senior associate reviews 10,000 documents, the recall rate can be increased to 80%, which is the standard that Judge Peck advocates.

[5.4.5.13] The EDRM, as explained in section 5.3.3, now includes a standard for Technology Assisted Review (which the EDRM names 'computer assisted review').[685]

Figure 2: Computer Assisted Review Reference Model



[5.4.5.14] Cormack and Grossman recently conducted a review of the best way in which the use of TAR should be conducted. The study looked at three types of TAR tools: Continuous Active Learning ('CAL'), Simple Active Learning ('SAL') and Simple Passive Learning ('SPL').[686] Essentially, all three use TAR to assist in 'training' the system to find relevant documents based on which documents the legal team code as 'relevant'. Each method uses a process whereby a set of documents (the 'training set'), say 1,000 documents, is coded

[685] Electronic Discovery Reference Model website: <http://www.edrm.net> at 11 September 2015.
[686] Gordon V. Cormack and Maura R. Grossman, *Evaluation of Machine-Learning Protocols for Technology-Assisted Review in Electronic Discovery*, at: <http://www.wlrk.com/webdocs/wlrknew/AttorneyPubs/WLRK.23339.14.pdf> at 11 September 2015.

by a senior lawyer as 'relevant' or 'not relevant' which the system then uses to 'learn' which other documents might be relevant as well. This process is repeated several times until the review team is satisfied that a sufficient level of relevant documents have been found. The difference between the three processes is whether randomly selected documents are used, or whether the set of documents has been located via a non-random method such as using basic keyword searching. In the CAL method, the 1,000 documents are selected using keyword searches and then the documents that are coded by the lawyer are used to train a learning algorithm, which scores each document in the collection by the likelihood of it being relevant. In SAL, the set of documents can be selected randomly or non-randomly, but then subsequent document sets for coding by the reviewer are selected based on those about which the learning algorithm is least certain. With SPL, the document set is selected randomly and relies on the review team to work on an iterative basis until there is some certainty that the review set is 'adequate'. The study concluded that when keyword searches are used to select all of the training sets, the result was superior to that achieved when a random selection is used, and summed up that 'random training tends to be biased in favour of commonly occurring types of relevant documents, at the expense of rare types. Non-random training can counter this bias by uncovering relevant examples of rare types of documents that would be unlikely to appear in a random sample'. Such studies are extremely valuable in learning how best to use this technology, however, further guidelines and endorsement from the courts would be welcome.

[5.4.5.15] These search technologies are crucial in assisting lawyers to find electronic evidence that is relevant, since any documents that are not relevant will not be admissible. Further, it is only relevant documents that must be authenticated and which would be subject to any of the exclusionary rules of evidence. Therefore, it is vital that relevant documents are located, and also any documents to which privilege applies so that these are not inadvertently discovered.

[5.4.5.16] It is submitted that the key to lawyers taking up the use of such technology, is through education, both at an undergraduate level, and for practitioners.

5.5 Privilege

[5.5.1.1] When providing documents as part of discovery, each party is entitled to make

a claim for legal professional privilege over documents to be discovered.[687] The doctrine of legal professional privilege is considered below. The protection of privilege is complicated in large data discovery because it can often be overlooked or missed in large datasets containing a large number of electronic documents.

5.5.2 Privilege at Common Law

[5.5.2.1] At common law, the doctrine of legal professional privilege protects from disclosure any oral or written statement, or other material, which has been created solely for the purpose of providing legal advice, or for the purpose of use in existing or anticipated litigation.[688] A claim for privilege may be established by evidence or by having regard to the nature or character of the documents themselves. In *Grant v Downs,*[689] the majority of the High Court, Stephen, Mason and Murphy JJ said 'it is for the party claiming privilege to show that the documents for which the claim is made are privileged. He may succeed in achieving this objective by pointing to the nature of the documents or by evidence describing the circumstances in which they were brought into existence. But it should not be thought that the privilege is necessarily or conclusively established by resort to any verbal formula or ritual.[690]

[5.5.2.2] In order to determine if a document is subject to legal professional privilege, the claimant must identify the purpose for which the document was created. If the sole purpose for its creation was to enable legal advice to be given, or for it to be used in existing or anticipated litigation, the document is, prima facie, subject to legal professional privilege. Legal professional privilege is concerned with communications, either oral, or written or recorded, and not with documents per se:[691]

> Where a document satisfies the common law test for legal professional privilege, any copy or copies of that document may also fall within the ambit of the protection afforded by the doctrine. It has been suggested that a copy of a privileged document which is brought into existence for a non-privileged purpose is itself privileged.[692]

---

[687] *Uniform Evidence Acts* ss 118 and 119 for client legal privilege.
[688] *Grant v Downs* (1976) 135 CLR 674, [682] and [688]-[689] (Stephen, Mason and Murphy JJ); *National Employers' Mutual General Insurance Association Ltd v Waind* (1979) 141 CLR 648, [654] (Mason J); *Baker v Campbell* (1983) 153 CLR 52, [60] (Gibbs CJ), [112] (Deane J), [122] (Dawson J); *Commissioner of Australian Federal Police v Propend Finance Pty Ltd* (1997) 188 CLR 501,[509] (Brennan CJ), [515] (Dawson J), and 550 (McHugh J).
[689] (1976) 135 CLR 674.
[690] Ibid 689.
[691] *Commissioner of Australian Federal Police v Propend Finance Pty Ltd* (1997) 188 CLR 501, [552] (McHugh J), [585] (Kirby J).
[692] *Brambles Holdings Ltd v Trade Practices Commission* (No 3) (1981) 58 FLR 452, [458] (Franki J).

[5.5.2.3] If a document contains purely legal advice, prima facie, it is privileged unless there is evidence to suggest that the copy was brought into existence for a purpose wholly unconnected with the purpose behind the creation of the original. At common law, legal professional privilege may attach to copies of non-privileged documents where those copies were brought into existence solely for use in obtaining legal advice, or for use in apprehended litigation.[693]

[5.5.2.4] Legal professional privilege is a rule of substantive law and not merely a rule of evidence. This means it is not confined to the giving of evidence in judicial proceedings, nor is it confined to processes of discovery and inspection. As an example of its potential width, legal professional privilege could be used to resist the giving of information or the production of documents to investigatory agencies such as the ASIC or ACCC.[694] This is explored further in section 5.5.8.

5.5.3 Privilege under the Uniform Evidence Acts

[5.5.3.1] The *Uniform Evidence Acts*, rename legal professional privilege as 'client legal privilege'.[695] The Acts also replace the 'sole purpose' test with a 'dominant purpose' test.[696] Client legal privilege is available to the 'client', as defined in the *Uniform Evidence Acts* s 117(1), and prevents evidence from being adduced if, on objection by the client, the court finds that adducing the evidence would result in disclosure of, inter alia, a confidential communication made between the client and the lawyer, or the contents of a confidential document prepared by the client or the lawyer. Client legal privilege is also available to an unrepresented party. The terms 'party', 'confidential communication' and 'confidential document' are all defined in *Uniform Evidence Acts* s 117(1).

[5.5.3.2] In summary, legal professional privilege attaches to preserve the confidentiality of communications between lawyer and client where they have been made or brought into existence for (a) the dominant purpose of that person seeking or being furnished with

[693] *Commissioner of Australian Federal Police v Propend Finance Pty Ltd* (1997) 188 CLR [501], [512] and [551] (Brennan CJ).
[694] *Daniels Corporation International v ACCC* (2002) 213 CLR 543.
[695] With respect to other statutory provisions: there is no equivalent of the *Uniform Evidence Act* provisions in *Evidence Act 1977* (Qld), *Evidence Act 1906* (WA) or *Evidence Act 1929* (SA), therefore the common law applies in those jurisdictions.
[696] *Evidence Act 1995* (Cth) ss 118;119, 120.

independent legal advice or services by a practising lawyer, or (b) the dominant purpose of preparing for existing or anticipated judicial or quasi-judicial proceedings.[697]

5.5.4 Waiver of privilege at common law

[5.5.4.1] At common law, waiver is imputed where the circumstances are such that it is unfair for the client to say that the privilege has not been waived.[698] What is unfair in the particular circumstances is determined by the conduct of the client. Waiver may be express or implied and it will be implied where it is considered that the particular conduct is inconsistent with the maintenance of the confidentiality that the privilege is intended to protect. In *Guinness Peat Properties Ltd v Fitzroy Robinson Partnership*,[699] a privileged document was inadvertently listed in the non-privileged part of the affidavit of documents and inspected and copied by the other side. The Court of Appeal in England held that a 'mere plea of inadvertence does not by itself necessarily enable a party to litigation to avoid a loss of privilege. Privilege may be lost by inadvertence'.[700] The court stressed the need for parties to take great care in preparing their lists of documents and providing inspection because ordinarily, a party who sees a document which has been listed or produced without a claim for privilege 'is fully entitled to assume that any privilege which might otherwise have been claimed has been waived'[701]. However, the court held that although the general rule was that once a document had been inspected it was too late to claim privilege, the court has a power to intervene under its equitable jurisdiction if either the inspection had been procured by fraud, or if the inspecting party realised, on inspection, that he had been permitted to see a confidential document only because of an obvious mistake.[702]

[5.5.4.2] One common form of implied waiver of privilege occurs where it would be unfair or misleading to allow a party to refer to or use material and yet assert that the material, or material associated with it, is privileged.[703] In such a case, the subjective intention of the party is irrelevant and the waiver arises because of some conduct on the privilege holder's part, which would make it unfair to allow it to maintain the privilege.[704] Another situation in which

[697] *Esso Australia Resources Ltd v Commissioner of Taxation* (1999) 201 CLR 49.
[698] Andrew Ligertwood, *Australian Evidence* (LexisNexis Butterworths, 4th ed, 2004), 296.
[699] [1987] 1 WLR 1027.
[700] Ibid 729, [11].
[701] Ibid 730.
[702] Ibid 731.
[703] *Attorney-General for the Northern Territory v Maurice* (1986) 161 CLR 475.
[704] Ibid [9].

waiver may be implied is where there has been no such conscious or voluntary act, only an inadvertent disclosure of privileged material.[705]

[5.5.4.3] The common law test focused on inconsistency, rather than fairness alone.[706] What brings about waiver is such a case is the inconsistency which the court, informed by considerations of fairness, perceives between the client's conduct and the maintenance of the privilege and 'not some overriding principle of fairness operating at large'. [707]

[5.5.4.4] With respect to electronic documents, in *GT Corporation Pty Ltd v Amare Safety Pty Ltd,*[708] one party, Amare, provided the other party, GT, with a number of forensic images. Amare later sought to claim legal professional privilege over documents contained on the forensic images. GT's lawyers subsequently looked at some of those documents and referred to a number of them in correspondence between the solicitors. Amare sought to claim privilege over the documents and restrain GT's lawyers from acting. Hollingworth J summed up how Australian courts apply the law where privileged documents have been inadvertently produced.[709] His Honour said that in determining what fairness requires in each case, the courts have had regard to such matters as (a) how the recipient obtained the document, (b) how quickly the party claiming privilege acted once it learned of the mistake, (c) what, if any, use had been made of the information, (d) what prejudice might flow to the other side from the waiver or non-waiver of privilege and (e) whether the inspecting party would have difficulty conducting the case whilst trying to ignore the content of the documents.[710] Hollingworth J found that there was no implied waiver of privilege in relation to the excluded material, as it had been disclosed through inadvertence. GT further sought an order compelling Amare to swear an affidavit describing every electronic document contained in the eight computer images over

[705] Ibid [10].
[706] *Mann v Carnell* (1999) 201 CLR 1, 29.
[707] Ibid 13. In *DSE (Holdings) Pty Ltd v Interan Inc* (2003) 127 FCR 499, Allsop J noted that by subordinating the notion of fairness to possible relevance in the assessment of the inconsistency between the act and the confidentiality of the communication, *Mann v Carnell* (1999) 201 CLR 1 produced an important change to the existing law. This approach was recently restated by the Federal Court in *SQMB v Minister for Immigration and Multicultural and Indigenous Affairs* (2004) 205 ALR 392, where it was found that waiver occurs 'when a party does something inconsistent with the confidentiality otherwise contained in the communication'.
[708] [2007] VSC 123 (25 May 2007). This case was decided by the Supreme Court of Victoria before the enactments of the *Evidence Act 2008* (Vic) so sets out the common law position.
[709] Ibid [12].
[710] *Hooker Corporation Ltd v Darling Harbour Authority* (1987) 9 NSWLR 538; *Meltend Pty Ltd v Rosenbaum and Restoration Clinics of Australia Pty Ltd & Marzola* (1997) 75 FCR 511; *Hongkong Bank of Australia Ltd v Murphy* [1993] 2 VR 419; *Key International Drilling Company Ltd v TNT Bulkships Operations Pty Ltd* [1989] WAR 280.

which Amare seeks to claim privilege, which Amare resisted. Hollingworth J ordered that Amare swear a further affidavit listing each and every document, including each attachment, contained it its electronic discovery in respect of which it wishes to claim privilege, with the affidavit also specifying the precise basis on which privilege is claimed.[711] With respect, Hollingworth J's decision is a sound one; how else is a party to know whether privilege can be claimed over documents unless each document is reviewed and assessed for privilege, in the same way it would be if the documents had been in hard copy.

5.5.5 Waiver of privilege under the Uniform Evidence Acts

[5.5.5.1] The *Uniform Evidence Acts* s 122 sets out the ways in which legal professional privilege can be lost, that is, where 'the party concerned has acted in a way that is inconsistent with the client or party objecting to the adducing of the evidence because it would result in a disclosure'. *Evidence Act 1995* (Cth) s 122 was amended by the *Evidence Amendment Act 2008* (Cth) which commenced in 1 January 2009, and *Evidence Act 1995* (Cth) s 122 was amended by the *Evidence Amendment Act 2007 (NSW)* which commenced 2 January 2009, to refer to actions that are inconsistent with the assertion of privilege, and these amendments were designed to bring the test for loss of client legal privilege in line with the decision in *Mann v Carnell*.[712] Prior to this, there was an inconsistency between common law waiver and waiver under the *Uniform Evidence Acts* and the ALRC, NSWLRC and VLRC had proposed that *Uniform Evidence Acts* s 122(2) be amended to allow that evidence may be adduced where a client or party has knowingly and voluntarily disclosed to another person the substance of the evidence or has otherwise acted in a manner inconsistent with the maintenance of the privilege.[713] The *Evidence Act 2008* (Vic) had already incorporated the inconsistency test in s 122. Tasmania[714] has retained the 'knowingly and voluntarily disclosed' test.

5.5.6 Inadvertent disclosure of privileged material

[5.5.6.1] A misunderstanding of the way in which electronic documents are stored as electronic data can lead to privileged material being inadvertently disclosed to the other side during discovery. A Compact Disc (CD) containing electronic evidence should not be

[711] *Guinness Peat Properties Ltd v Fitzroy Robinson Partnership* [1987] 1 WLR 1027, [81].
[712] (1999) 201 CLR 1, [29].
[713] Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Review of the Uniform Evidence Acts*, ALRC DP 69, VLRC DP (2005) [13.5].
[714] *Evidence Act 2001* (Tas) s 122(2).

discovered as 'a CD of electronic files', without each individual file on the CD being reviewed for potentially privileged documents (for that matter, irrelevant documents should not be discovered). Similarly, a hard disk of electronic files should not be discovered for the same reason. It is also imperative that lawyers understand exactly what is being discovered and a review of the information being discovered should be undertaken. In *GT Corporation Pty Ltd v Amare Safety Pty Ltd*,[715] the defendant discovered eight forensic images in their entirety without first reviewing what each forensic image contained. The question of what constitutes a 'document' has already been considered in sections 4.2 and 4.3. The consequences of inadvertent discovery of privileged documents is examined further below.

[5.5.6.2] A recent decision highlights how it is easy for paralegals to miss privileged documents during a subjective review of documents for discovery. In *Expense Reduction Analysts Group Pty Ltd v Armstrong Strategic Management and Marketing Pty Limited*[716] orders were made by the Equity Division of the Supreme Court of New South Wales for general discovery which required Norton Rose (representing the defendants) to review approximately 60,000 documents. An electronic online database, known as 'Ringtail' was used to identify and categorise the documents. Entries were made which indicated whether each document was relevant or subject to legal professional privilege. Following the review, relevant documents were discovered, and privileged documents were listed, but not provided. In December 2011, Norton Rose wrote to Marque Lawyers (representing the plaintiffs) indicating they had 'inadvertently' failed to claim privilege in respect of privileged documents. Marque Lawyers failed to return the documents, arguing privilege had been waived. The key issue that arose was whether the defendants had waived their claim of privilege over the documents, and this issue went all the way to the High Court of Australia. At first instance Bergin CJ in Eq held that Norton Rose had intended to claim privilege over the documents in question and accordingly, these documents were discovered inadvertently. The Court of Appeal overturned this decision. On appeal to the High Court, the High Court referred to the primary judge's acceptance of the reviewers evidence that they would not have made an error in deciding whether the documents were privileged or not, rather that they failed to properly manipulate the electronic system. Her Honour's view was that absent a finding of mistake, disclosure would amount to a waiver of privilege not to produce them, therefore, in order to establish that

[715] [2007] VSC 123 (25 May 2007).
[716] (2013) 250 CLR 303.

discovery was inadvertent, it had to be first be shown that the reviewers had actually intended to claim privilege over the documents, to determine if a mistake had been made. The fact that duplicates of documents inadvertently disclosed had been included in the privileged section of the List of Documents demonstrated that the disclosure was inadvertent. The High Court reviewed the approach of the English courts in *Guinness Peat Properties Ltd v Fitzroy Robinson Partnership*[717] and noted that 'although discovery is an inherently intrusive process, it is not intended that it be allowed to affect a person's entitlement to maintain the confidentiality of documents where the law allows. It follows that where a privileged document is inadvertently disclosed, the court should ordinarily permit the correction of that mistake and order the return of the document, if the party receiving the documents refuses to do so.'[718] The court was of the view that today, in large commercial cases, mistakes are now more likely to occur and referred to the case of *ISTIL Group Inc v Zahoor,*[719] where Lawrence Collins J observed that '[t]he combination of the increase in heavy litigation conducted by large teams of lawyers of varying experience and the indiscriminate use of photocopying has increased the risk of privileged documents being disclosed by mistake.'[720] With respect, the court did not talk about the use of tools such as Technology Assisted Review which assists law firms to move away from traditional and expensive methods of review. Technology Assisted Review is examined in detail in section 5.4.5.

[5.5.6.3] The High Court noted that the courts will normally only permit an error to be corrected if a party acts promptly. If the party to whom the documents have been disclosed has been placed in a position, as a result of the disclosure, where it would be unfair to order the return of the privileged documents, relief may be refused. However, in taking such considerations (analogous to equitable considerations) into account, no narrow view is likely to be taken of the ability of a party, or the party's lawyers, to put any knowledge gained to one side. That must be so in the conduct of complex litigation unless the documents assume particular importance.[721] The High Court also went on to provide a strongly worded rebuke to the solicitors who did not return the privileged material when requested to do so, pointing out that it remains an ethical obligation to do so, and the it is solicitor's duty to meet the objectives

[717] [1987] 1 WLR 1027.
[718] *Expense Reduction Analysts Group Pty Ltd v Armstrong Strategic Management and Marketing Pty Limited* (2013) 250 CLR 303 [45].
[719] [2003] 2 All ER 252.
[720] Ibid [72].
[721] Ibid [49].

of the *Civil Procedure Act 1997* (Eng) to ensure the 'just, quick and cheap resolution of the real issues in the dispute or proceedings'. With electronic discovery, the tools now exist that can allow a set of documents, such as those identified as privileged, to be compared with other documents in the review set, to determine it there might be others that are privileged.

5.5.7 Non-waiver of Privilege or 'clawback'

[5.5.7.1] The United States of America has responded to the risk of exposing privileged documents in the sheer volume of electronic documents with 'clawback' agreements, or non-waiver of privilege agreements. These agreements are designed to allow parties to conduct a less rigorous privilege review prior to production, while providing that if privileged materials are produced, they can be reclaimed without any waiver occurring. These agreements may provide that the inadvertent production of materials shall not constitute a waiver of any applicable privilege, so long as the privilege is asserted within a reasonable time after the inadvertent production is discovered or they may contain a set of defined procedures for asserting post-production claims of privilege. Amendments in 2006 to the *Federal Rules of Civil Procedure* (USA) provide for parties to make such agreements. If information is produced during discovery that is subject to a claim of privilege, then the party making the claim can notify the other party in which case the party must return, sequester or destroy the information and may not use the information.[722] Such agreements may bind the parties in the case but not third parties.

[5.5.7.2] The *Federal Rules of Civil Procedure* (USA) work in conjunction with the *Federal Rules of Evidence* (USA), to cover an instance where there is inadvertent disclosure and where the party took steps to notify the other party promptly. [723]

[5.5.7.3] In Australia, *Federal Court of Australia Practice Note CM6* provides a Pre-Discovery Checklist where the parties are to agree upon the strategies they will use to manage documents that are subject to a claim of privilege or confidentiality. *Supreme Court of New South Wales Practice Note SC Eq 3*[724] s 29 provides for practitioners to agree on whether ESI is to be discovered on a without prejudice basis, that is without prejudice to an entitlement to subsequently claim privilege over any information that has been discovered and 'is claimed to

[722] *Federal Rules of Evidence* (USA), r 5(B).
[723] *Federal Rules of Evidence* (USA) Article V. Privileges, r 502 (2014).
[724] Australia, Supreme Court of New South Wales, *Practice Note SC Eq 3*, 10 December 2008.

be privileged under s.118 and/or s.119 of the *Evidence Act 1995* (NSW) and/or at common law'.

5.5.8 Privilege in Federal investigations

[5.5.8.1] Preserving privilege in documents that are obtained by way of seizure can be difficult, especially as there appear to be little guidelines for those granted orders to seize. The Australian Law Reform Commission ('ALRC') released its report, 'Privilege in Perspective: Client Legal Privilege in Federal Investigations'[725] on 13 February 2008. The focus of the ALRC's inquiry was on the application of client legal privilege in the context of federal investigations and Royal Commissions of inquiry. During the *Oil-for-Food Inquiry* heard before Commissioner Terence Cole QC in 2006, extensive claims for privilege were asserted by the Australian Wheat Board. Commissioner Cole considered that these claims generated a conflict between the public interest in discovery of the truth and the fundamental right of persons to obtain legal advice under conditions of confidentiality.[726]

[5.5.8.2] In recent decades, the number of federal bodies with coercive information-gathering powers has grown significantly, such bodies include the Australian Federal Police (AFP), the Australian Taxation Office (ATO), the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC).

[5.5.8.3] In relation to the application of client legal privilege to federal bodies with coercive information-gathering powers, the Terms of Reference required the ALRC to consider whether it would be desirable to (a) modify or abrogate the privilege in some areas in order to achieve more effective performance of Commonwealth investigatory functions; (b) clarify existing provisions for the modification or abrogation of the privilege, with a view to harmonising them across the Commonwealth statute book; and (c) introduce or clarify other statutory safeguards where the privilege is modified or abrogated, with a view to harmonising them across the Commonwealth statute book. [727]

[5.5.8.4] The ALRC recommended that legislation should be enacted to cover various aspects of the law and procedure governing client legal privilege claims in federal

[725] Australian Law Reform Commission, *Privilege in Perspective: Client Legal Privilege in Federal Investigations*, Report 107 (2007).
[726] Ibid [1.6].
[727] Ibid [1.8].

investigations.[728] The ALRC also recommended that federal client legal privilege legislation should provide that, in the absence of any clear, express statutory statement to the contrary, client legal privilege applies to the coercive information-gathering powers of federal bodies,[729] and any such legislation should take into account several factors when determining whether client legal privilege may be abrogated and these should include (a) the subject of the investigation, including whether the inquiry concerns a matter/s of major public importance that has a significant impact on the community in general or on a section of the community, or is a covert investigation, (b) whether the information sought can be obtained in a timely and complete way by using alternative means that do not require abrogation of client legal privilege, and especially (c) the degree to which a lack of access to the privileged information will hamper or frustrate the operation of the investigation and whether the legal advice itself is central to the issues being considered by the investigation.

[5.5.8.5] In *TLC Consulting Services Pty Ltd v Paul Michael White*,[730] as almost an afterthought at the end of the judgment, the court added that if in examining the mirror copy of the hard drive of the server, the officers of the appellant identified a document to which legal professional privilege would reasonably be considered to apply, the officers will not further examine the document. With respect, this puts the obligation regarding privilege on the party receiving the information, rather than the producing party. The receiving party often will not have the expertise or knowledge to identify privileged material. Further, the party receiving the material is the very party who should not be privy to seeing the privileged material.

[5.5.8.6] An example of the inconsistency and misunderstanding of retrieval and review of material on electronic media containing possibly privileged material was highlighted during a 2012 Queensland Parliamentary Inquiry (QPI) into the public release of confidential Fitzgerald Inquiry documents,[731] where the Crime and Misconduct Commission's IT Manager, was strongly questioned under oath over his inability to retrieve certain information about internal emails requested under a summons. This interrogation of the IT Manager highlights the fundamental misunderstanding of the nature of electronic records, and how information is

[728] Ibid ss 5, 6.
[729] Ibid.
[730] [2003] QCA 131 (21 March 2003).
[731] Queensland Parliamentary Crime and Corruption Committee, Inquiry into the CMC's release and destruction of Fitzgerald inquiry documents, hearings conducted on Wednesday 13 March to Friday 22 March, and on Thursday 28 March 2013, <https://www.parliament.qld.gov.au/work-of-committees/committees/PCCC/inquiries/past-inquiries/FitzgeraldDocuments>, as at 5 January 2016.

being archived and stored without capturing the 'original' document, without all of its metadata intact. Further, it highlights how IT Managers are being expected to deal with evidence, without any real guidance as to what they need to do. The email in question was a draft email that had been created by the Crime and Misconduct Commission's General Counsel in 2012 and the version that was produced to the QPI was a printout, which meant the IT Manager, without the benefit of the metadata from the original electronic file, was unable to determine if the printout came from TRIM, the CMC's archive system, or from General Counsel's Draft folder directly from their email repository. The IT Manager attempted to retrieve the email from repositories restored from backup tapes, and was unable to retrieve the time stamp from the restored emails. During the QPI, the State Member for Redlands in the Queensland Parliament, Peter Dowling MP criticised the IT Manager for not obtaining the email directly from the General Counsel's online email and the IT Manager responded that he did not have the right to do so, because he was not authorised to access the General Counsel's email. The MP's criticism was directed at the fact that a summons had been issued and that in itself gave the IT Manager the authority to access what he needed. The IT Manager said if he had done so, it would have given him access to information outside the scope of the summons.[732]

[5.5.8.7] In the United States of America, the courts have determined that the expertise of ISP technicians to conduct a search pursuant to a warrant faxed to them by a government agent, is far superior to that of the agents.[733]

[5.5.8.8] In Canada, the courts do recognise that a server contains many documents which need to be reviewed for privilege. In *National Bank Financial Ltd v Potter*,[734] the bank's counsel obtained a computer server belonging to the defendant, which contained privileged documents. The court upheld an application to remove the bank's counsel from the record as they had wrongfully accessed and reviewed the privileged documents. Scanlon J stated that counsel should have stopped any review and sought direction from the court as soon as they knew or reasonably suspected they had acquired privileged material. Scanlon J dismissed the bank's argument that privilege was lost due to a lack of expectation of privacy for emails

[732] Bill Dawes, *Queensland MPs call for independent inquiry over Fitzgerald files shambles*, Image & Data Manager, March-April 2013 at 20.
[733] In *U.S. v Bach*, 310 F.3d 1063 (8th Cir. 2002) cert. denied, 538 U.S. 993 (2003), ISP technicians searched the defendant's e-mail account for child pornography pursuant to a warrant faxed to them by a government agent. Further, evidence obtained via a search of a seized computer several weeks after the search warrant has expired, is still admissible: *U.S. v Hernandez*, 183 F. Supp 2d 468 (D.P.R 2002).
[734] [2005] N.S.J. No. 186 (N.S.S.C) (QL).

contained on a server comparing the computer server to a law firm's filing cabinet. Likewise, in *Celanese Canada Inc. v Murray Demolition Corp,*[735] a large volume of documents were seized from a defendant pursuant to an Anton Piller order. Contrary to the order, a complete list of documents seized was not made prior to removal from the premises and 1,500 electronic documents that had not been screened for privilege claims were downloaded onto a portable hard-drive and copied onto CD-Roms and uploaded onto the computers of the plaintiff's solicitors unknown to the defendant. In this case, it was held that a list should have been made of each of the documents on the hard drive and CD-Roms. Moreover, in *Roeske v Grady*[736] the defendant applied for an order that the plaintiff produce her PowerBook computer including but not limited to the computer hard drive and any removable floppy, CD or other DVD disks containing data from that computer. This included a proposal for the production of the information on the hard drive. A forensic computer expert would make a forensic image of the data, conducted a by-category analysis of the information and provide information in certain limited categories to counsel for the defendant. The court denied the application for the production of the hard drive taking into consideration the marginal value of the hard drive for trial purposes.

[5.5.8.9] The courts appear to recognise the problem with receiving parties dealing with privileged material and often decline to provide orders for production if the probative value of the material is minimal. However, the courts do not go so far as to provide guidance to receiving parties on how to handle material that may contain privileged documents.

5.5.9 Privilege and Electronic Documents

[5.5.9.1] This section 5.5 highlights the need to determine privilege before discovery is given, and evidence is prepared for tender to any court. If hard drives are classified as documents, this can cause serious consequences for those charged with reviewing the material on the hard drive. The case of *GT Corporation v Amare*[737] highlights this very problem, where a hard drive was discovered containing privileged documents that had not been reviewed.

[5.5.9.2] Perhaps the largest factor that points to issues with electronic documentary evidence is when privilege is considered. In section 4.3, the fact that a hard drive can be

[735] 2006 SCC 36.
[736] 2006 BCSC 1975 (CanLII).
[737] [2007] VSC 123 (25 May 2007).

classified as a document is inconsistent with the reality that a hard drive can contain many thousands, if not millions, of documents, all of which have to be reviewed for relevance and most importantly, for privilege. The case of *GT Corporation v Amare,*[738] as summarised in section 5.5.4, demonstrates the problems when a hard drive is simply handed over during discovery, without a thorough review of the content to determine if any documents contained on the hard drive are indeed privileged.

[5.5.9.3] If a hard drive is seized either by a regulatory authority pursuant to a seizure warrant, or via an Anton Piller order, how are privileged documents identified and by whom? The factor in hard drives that have been seized is that the one in possession of it is the one who by rights, should not view the privileged material.

[5.5.9.4] Presently, there is no framework in place in Australia as to who is responsible for reviewing the hard drive for privileged or confidential documents and it has been left up to the courts to order that an independent third party, usually a computer forensics expert, to review the material. In New Zealand, the court has allowed an independent barrister to assist the independent forensic expert to determine which documents are privileged.[739]

[5.5.9.5] However, there have been cases, such as the QPI matter where an IT Manager was not only under qualified to retrieve and review information, but was criticised for not finding the correct information, notwithstanding the IT Manager had no legal qualifications nor any training on evidentiary procedure. The problem lies in that the rules surrounding electronic evidence are unclear, there is very little judicial guidance on what constitutes a 'document', and exactly how records are to be kept and retrieved. Further, summonses or other court orders that allow access to be gained to repositories of electronic information, need to be clear about how to deal with documents that are not part of the summons. This is the case whether it is private, confidential or privileged material, and is a common problem for regulatory bodies that seize computer hard drives.

[5.5.9.6] As considered above in section 4.2, under the *Uniform Evidence Acts*, a 'document' is defined quite broadly and case law has confirmed that items such as CD-Roms, hard drives, forensic images and the like can constitute a 'document'. Therefore, if access can

[738] Ibid.
[739] *Chief Executive of the Ministry of Fisheries v United Fisheries Ltd* [2010] NZCA 356; [2011] NZAR 54 (6 August 2010) at [70] per Baragwanath J.

be obtained to a 'document' that is a hard drive, but in reality that hard drive contains hundreds of thousands of documents, how is the person trying to retrieve one document only, supposed to deal with the other documents, for which they are potentially not qualified to deal with?

[5.5.9.7] In the Queensland Parliamentary Inquiry[740] referred to in [5.5.8.6] above, reference was made to computer forensic specialists and whether such an expert should have been used to retrieve the email in question. A computer forensic specialist would certainly be well qualified to deal with the evidence, and retrieve the document in question, however, if records were stored appropriately in the first place, and/or if the summons had made it clear how the person to whom the summons was directed was to handle information not relevant to the summons, then a computer forensic expert would not be required. Further, computer forensic experts are generally expensive to retain and there must be a better framework in which to operate so that organisations do not need to be put to such expense each time specific information needs to be accessed. It seems clear that the email in question had been entered into the CMS's TRIM records management system. Therefore, why was the email not simply obtained from TRIM, rather than having to resort to backup tapes? Further, if it was obtained from TRIM, then the document should have been archived in such a way as to preserve the integrity of the original metadata, thereby ensuring that the information required, that is, the date stamp, was visible. If this information was not available, then the whole records management process should be called into question, as the original document has most likely been changed.

[5.5.9.8] With respect, IT Managers are too often required to perform the work of evidential experts, for which they have little or no training. If they are required to search repositories under their management, then (a) the system needs to be such that information is stored properly and appropriately so retrieval is done in a correct manner and (b) the summons itself should clearly set out how information stored in a 'system' to is be handled, when it is not relevant to the summons. There appears to be an urgent need for legal rules to treat electronic records in a different light from paper records, in that electronic records more often than not, reside in a system. How records are stored and retrieved and viewed as evidence, should be considered in light of the system itself, not a 'document' in isolation. In this example,

[740] Queensland Parliamentary Crime and Corruption Committee, Inquiry into the CMC's release and destruction of Fitzgerald inquiry documents, above n 731.

the IT Manager could be forced to review privileged documents, for which the IT Manager has no training, nor is expected to know what privilege might be.

5.6 Producing Electronic Evidence

[5.6.1.1] In order to produce a document in court, it is normally produced through a witness who is in court. The witness can identify the document and explain its relevance and significance to the case. The document is not yet in evidence, it has only been made available for inspection. After a document has been produced for inspection, the party seeking to tender it as evidence, needs to establish its relevance and its admissibility. If the document bears the witness's signature and the witness verifies that signature in court, then it is admissible and the Hearsay Rule does not apply, as it is evidence of the witness and is not a statement from outside of the court. Otherwise, one of the exceptions to the Hearsay Rule must apply. Once a document has been tendered and admitted into evidence, it is in the court's discretion as to the weight to be given to that evidence.

[5.6.1.2] A lengthy process precedes the production of documents in court. Each court practice note sets out its requirements for production of documents during discovery and at trial. The *Federal Court of Australia Practice Note CM6* encourages exchanging electronically sourced information ('ESI') in native format where agreed or as searchable images.[741] Native files are to be converted directly to PDF format in order to preserve text searchability (as opposed to converting to TIFF format where text searchability is lost and to be regained, the documents must be processed through Optical Character Recognition software). The *Supreme Court of New South Wales Practice Note No. SC Gen 7* provides that 'discovery of electronically stored documents and information is to be made electronically', however, does not prescribe the format in which documents are to be exchanged. Hard copy documents are imaged and data coded for exchange in an electronic discovery. ESI, however, is already in an electronic format, so the questions for litigants to answer is, in what format should electronic documents be exchanged? Should they be exchanged in an image format, or in the document's native format?

[5.6.1.3] Typically, documents that are exchanged during an electronic discovery are

[741] Australia, Federal Court of Australia, Practice Note CM6 *The Use of Technology in the Management of Discovery and the Conduct of Litigation*, 29 January 2009.

those that can easily be read using their native application, and such 'standard' documents would include Microsoft Office documents (such as MS Word, MS Excel), Adobe PDF, image formats such as JPG, GIF, TIFF, emails in MSG or EML format (attachments to emails will generally be in one of the other 'standard' formats). Non-standard documents include those that require specialist software (software that you would not typically find in a standard office environment, or a standard environment particular to the parties to the matter). Standard files are typically converted to an image format, to ensure that each page becomes finite with the result being that if evidence is tendered in court, then print-outs of the electronic files can always be referred back to the electronic version of the document (which would simply not be possible if the documents were printed without a unique page identifier on each page). Each page should be electronically stamped with a unique page identifier in accordance with the relevant court practice direction and/or agreed protocol between the parties. As set out in [5.3.4.3], *Federal Court of Australia Practice Note CM6* makes reference to the exchange of documents in native format. The exchange format for documents during discovery is determined by court practice notes.[742]

[5.6.1.4] In hard copy discovery, discovery lists are exchanged, and the hard copy documents are made available for the other side to inspect. With electronic discovery, the discovery list can be exchanged, or instead the metadata collected from the electronic files, together with the files themselves, can be exchanged in the agreed format. Specialist legal review software is then used to review the documents.

5.7 Presentation of Evidence at Trial

[5.7.1.1] Electronic trials have been in operation for since the early 1990s, however are still primarily used for larger, document heavy trials. Although courts are slowly installing computer equipment whenever new courtrooms are built, it is still rare that a trial is run in a paper less, or 'less paper' manner.

[5.7.1.2] An electronic trial is one where the documents are all available electronically

[742] For example, the exchange format can be a four-table Access database, as set out in the Advanced Document Management Protocol which accompanies Australia, Federal Court of Australia, *Practice Note CM6 The Use of Technology in the Management of Discovery and the Conduct of Litigation*, 29 January 2009, or it may be a Comma Separated Value (CSV) text file, or it may be a spreadsheet, as specified in Supreme Court of Queensland's Practice Note No. 10 of 2011 - *Use of Technology for the Efficient Management of Documents in Litigation*.

via online systems, directly to the court, and where the documents themselves can be displayed electronically to those in the courtroom. The benefits of electronic trials are that they can save an inordinate amount of time as the lawyers involved in the hearing do not have to spend time finding each individual page being referred during the hearing, as the document is available on screen within seconds of counsel referring to the document identifier. An electronic trial comprises equipment, services and software and can be undertaken by agreement of the parties or by an order of the court.[743] Electronic trials can be used where sensitive documents need to be kept secure[744] and orders to run the trial electronically should be sought as early as possible in the proceedings.[745] Transcripts can be provided electronically, which means they can be searches and marked up electronically, and can be cross referenced to other documents.

[5.7.1.3] Electronic trials are still relatively uncommon; the main reason being that practitioners are not yet well versed in how to run an electronic trial. Indeed, many judges and counsel still prefer to have paper on hand when cross examining witnesses and this is understandable; one does not practice a certain way for years and decide to change suddenly.[746] On the other hand, some counsel prefer the benefits that technology brings to trial preparation and evidence presentation. The ability to make notes on documents electronically, access documents from anywhere without the need to carry around huge volumes of hard copy documents certainly has its appeal.

[5.7.1.4] As electronic documents continue to be discovered in their 'native' electronic format, it is speculated that electronic trials will become more common. In the future, all trials will be conducted using electronic versions of the documents, rather than hard copy, and the use of technology such as social media will be used to correspond with the courts to obtain interlocutory orders, rather than going to the expense of appearing in court. Documents will be able to be uploaded to the courts at the click of a button, and the judge will be able to be

[743] *Idoport v National Australia Bank Ltd* [2000] NSWSC 338; in that case Einstein J held that the power to order use of technology at trial was contained within the inherent jurisdiction of the court; His Honour also referred to the overriding purpose and made reference to the Lord Wolf reforms; *Harris Scarfe v Ernst & Young (No 3)* [2005] SASC 407. In *Harris Scarfe v Ernst & Young (No 3)*, Bleby J held that he was satisfied that rules of court gave him specific power to make orders for the use of technology at trial.

[744] *Seven Network Ltd v News Ltd (No 9)* [2005] FCA 1394.

[745] *Kennedy Taylor (Vic) Pty Ltd v Grocon Pty Ltd* [2002] VSC 32.

[746] The Hon. Justice Chesterman, *Managing Complex Litigation*, (Speech delivered at the Queensland Law Society's Continuing Legal Education Program, Brisbane, 22 October 2003); <http://www.sclqld.org.au/judicial-papers/judicial-profiles/profiles/rnchesterman/papers/1>, at 11 September 2015.

directed to documents and portions of documents at the click of a mouse. Indeed, the Chief Justice of Victoria recently announced that the Victorian Courts are moving towards being paperless by 2016 and that the courts intended to make more use of social media.[747]

[5.7.1.5] Technology makes every step leading up to and during trial much more time and cost effective, from reviewing and discovering documents, producing them in the courtroom and accessing transcripts. Electronic trials save time in the courtroom, by allowing documents to be displayed quickly and by enabling documents to be searched and retrieved quickly. Hyperlinks between documents such as witness statements and their exhibits, means it is much more efficient for the judge hearing the matter to review documents.[748]

[5.7.1.6] Electronic trials provide a complete service for parties including structuring and uploading an electronic courtbook, ensuring all parties and the judge have access to the software in and out of court, publishing documents electronically in court, providing a real-time transcript service, and hyperlinking and indexing documents to increase accessibility. The main advantage of courtroom technology is that it is possible for parties to work externally from the courtroom but still be able to login and the documents published in the courtroom, along with the transcript in real-time to know exactly what is going on at any time. Users also have access to indexes including hyperlinked lists of each day's published documents and documents from each witness. A Court Operator locates and displays documents referred to by counsel, and this saves having to produce multiple copies of documents for our counsel, witnesses and the judge, thereby saving an inordinate amount of time and costs during the hearing. Video conferencing is available for witnesses to provide testimony remotely, if they are unable to travel to court.

[5.7.1.7] Electronic transcript can be made available to the parties and to the court, although in many large matters, real time transcript is used, which is where the text of the transcript is available on screens in the hearing room, or even remotely back at the parties' offices, seconds after the witness has spoken. Transcript analysis tools then enable notes and issue to be marked on the transcript, thereby enabling the evening's review of the transcript to be much more efficient, as notes are already available on the transcript. Although not yet

[747] The Hon. Marilyn Warren AC, The Litigation Contract: The Future Roles of Judges, Counsel and Lawyers in Litigation, Victorian Bar & Law Institute of Victoria Joint Conference High Stakes Law in Practice and the Courts, Friday 17 October 2014.
[748] Federal Court of Australia Practice Note CM6 makes reference to electronic trials being more cost effective.

widely use, video transcript can be used, which can link between the video, audio and transcribed text.

[5.7.1.8] Electronic trials can certainly be used for smaller matters,[749] which can realise the same time and cost savings on a proportionate basis compared to large matters. If parties have a small number of documents, yet they are in electronic format, then a very simple display system can be made available in the courtroom. Counsel presenting the material can bring up a document on their screen, which will then show up on all screens around the room. Alternatively, a court operator may be engaged to bring up and display the documents.

[5.7.1.9] The benefits of using an electronic trial in a small matter are the same benefits as those in more complex matters, that is, they result in the display of documents much more quickly, allowing those present in the courtroom to view the documents quickly and easily, without the need for each party to go to cumbersome hard copies and wait for everyone else to be 'on the same page', and this leads to shorter trials.

[5.7.1.10] Discovery in smaller matters is now being prepared electronically, not necessarily because the lawyers undertake it in this way, but because the documentary evidence exists only in electronic format. It makes sense to use technology to find the relevant electronic documents, then discover them electronically and then of course, to provide them to the court electronically. Smaller claims are still presented with large volumes of electronic documents to review, and this is where tools to find those documents relevant to the issues are necessary, as they save costs.

[5.7.1.11] It is now becoming more common to provide electronic briefs to counsel and if counsel review and prepare evidence electronically, this aids counsel being able to run the trial electronically. Briefs can contain links to the documents as they are referenced in the brief.

[5.7.1.12] Each Australian jurisdiction does have a practice note encouraging the parties to exchange documents during discovery electronically, and *Federal Court of Australia Practice Note CM6* contains a Pre-Trial Checklist. Since almost all evidence is created electronically, electronic discovery is now the only way to deal with electronic evidence. Technology now enables 'predictive' coding and 'concept searching' which allow lawyers to

[749] *Visa International Service Association v Reserve Bank of Australia* [2003] FCA 977.

find relevant documents in very large repositories of data. The technology is improving all the time and the cost is decreasing as the use of such technology becomes more wide spread.

[5.7.1.13] All material will need to be available to the court electronically, whether they be simple, small matters, or large, complex matters. The starting point is filing documents electronically. Few courts still provide electronic filing capabilities and if they do, this extends to the originating proceeding and perhaps some of the pleadings. Documentary evidence is generally presented during the hearing and often handed up in hard copy. In the future, there will be the ability for lawyers to upload evidence to the court beforehand, so evidence can be presented to the court from a virtual location, much in the same way as documents are uploaded to various repositories in the Cloud for retrieval at the moment.

[5.7.1.14] It is speculated that courtrooms of the future will be equipped with basic equipment such as monitors for display, internet connectivity so documents can be accessed from within the courtroom and/or remotely. Documentary evidence will be available electronically, so as witness statements and affidavits are prepared, these will automatically link to the image or "native" file for the document. Electronic transcripts will be available and if transcribed, will be cross referenced to the video, audio and text of the transcript. Video conferencing, although widely used now, will be available for those witnesses who are unable to travel long distances and are able to appear remotely, and the use of streaming video across the internet means cost effective video is much more accessible. Judges will interact with parties using technology currently used in social media, with access permissions determined by the court. Interlocutory orders, submissions and so on, will all be able to be uploaded to the court site, and links will be made available to documents, or parts of documents, for the judge to review. In this way, the judge can have full access to the case, see all material in relation to the case, and a full audit history of what has transpired. This will be particularly useful if parties change and the judge hearing the matter is different to the judge who heard interlocutory matters. The end result will be the more efficient use of technology to enable documents to be accessed quickly and easily, with cost savings to the litigant.

5.8 Adducing Evidence

[5.8.1.1] At the time evidence is tendered in court, the court must decide whether the evidence is admissible. The *Uniform Evidence Acts* draw a distinction between ways of adducing evidence and the admissibility of evidence.[750] Evidence of the contents of a document, may be or may include evidence of a representation by a person about an asserted fact.[751] Consequently, some or all of the contents of a document, although adduced in evidence in accordance with *Uniform Evidence Acts* s 48(1), may be inadmissible as hearsay, unless an exception to the Hearsay Rule is available.

[5.8.1.2] The common law 'original document' rule has been abolished by *Uniform Evidence Acts* s 51 and instead, the *Uniform Evidence Acts* facilitate the process of adducing evidence of the contents of a document where something other than the original document is tendered pursuant to *Uniform Evidence Acts* s 48.

[5.8.1.3] *Uniform Evidence Acts* s 48 permits evidence of the contents of a 'document in question' (defined ins 47(1)) to be adduced by various methods, which include tendering a copy (s 48(1)(b)), tendering a document produced from electronically-stored information (s 48(1)(d)) and tendering a document that forms part of the records kept by a business and purports to be a copy of the document in question (s 48(1)(e)). However, s 51 has not abolished or affected the need to prove that the document tendered is the document it purports to be, and s 48(1) has not authorised the adducing of evidence merely by tendering a document in the absence of any evidence establishing what the document was. Section 48(1) merely prescribes the means of adducing evidence of the contents of documents and leaves untouched the need to establish their authenticity.

[5.8.1.4] The authentication of documents should be distinguished from relevance, the procedure for proving the contents of documents, and admissibility of representations in documents as business records notwithstanding the Hearsay Rule.[752]

[750] *Uniform Evidence Acts* Part 2.2.
[751] *Uniform Evidence Acts* s 48(1).
[752] *National Australia Bank Ltd v Rusu* (1999) 47 NSWLR 309 [312] (Bryson J).

5.9 Summary & Conclusion

[5.9.1.1] The questions to be answered following an analysis of discovery procedures are:

Question 4:
Does the discovery process provide sufficient safeguards to ensure that the integrity of evidence remains intact?

Question 5:
For documents to which legal professional privilege applies, are there sufficient protection measures in place for retrieval of evidence on electronic media that contains privileged information?

6. THE AUTHENTICATION OF ELECTRONIC EVIDENCE

[6.1.1.1] Authenticity of an electronic document can be called into question by challenging the provenance of the document, that is, that the proponent has not provided sufficient evidence to show how the electronic evidence came into existence. This can include (a) a claim that the records were altered, manipulated or damaged between creation and tender in court, (b) that the reliability of computer program is in question; and (c) the identity of the author is in question.[753]

[6.1.1.2] With electronic evidence being so very different to paper, as described in Chapter 3, how have the cases to date dealt with authenticating electronic evidence? The Director of the Center for 21st Century Security and Intelligence at Brookings Institution, Peter W. Singer stated that 'ninety-seven percent of Fortune 500 companies have been hacked … and likely the other 3% have too, they just don't know it.'[754] This does not necessarily mean that every computer that has information on it, has had information changed or content altered, however, it does mean that the authenticity of a document created on a computer system does need to be questioned given the risk that unknown and undetectable changes may have been made to a document.

[6.1.1.3] Before a document, including a business record, is admitted in evidence, it is necessary that there should be an evidentiary basis for finding that it is what it purports to be.[755] Ordinarily, documents are not taken to prove themselves, although there are exceptions such as public registers and certified documents.[756]

6.2 The Requirement to Authenticate in Australia

[6.2.1.1] In Australia, in order to be admitted, evidence must be relevant.[757] Pursuant to *Uniform Evidence Acts* s 58(1), if a question arises as to the relevance of a document or thing, the court may examine it and may draw any reasonable inference from it, including an inference

[753] *Nobel Resources SA v Gross* [2009] EWHC 1435 (Comm).
[754] Peter Singer & Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2009).
[755] *National Australia Bank Ltd v Rusu* (1999) 47 NSWLR 309, 312 (Bryson J).
[756] Ibid.
[757] In *Australian Competition and Consumer Commission v Air New Zealand Ltd* (No 2) [2012] FCA 1355 (30 November 2012), Perram J stated that 'there is no provision of the *Evidence Act* which requires that only authentic documents be admitted into evidence. The requirement for admissibility under the Act is that evidence be relevant, not that it be authentic. On some occasions, the fact that a document is not authentic will be what makes it relevant, ie, in a forgery prosecution.'

as to its authenticity or identity. A document cannot authenticate itself.[758] Therefore, a party seeking to rely on a document must adduce evidence that confirms that the document is what it purports to be or what the party claims it to be. This applies whether a document is being admitted through a witness, or through one of the exceptions to the Hearsay Rule, such as the Business Records Exception.

[6.2.1.2] The evidence required to authenticate a document will be determined in part by the nature of the document in issue. A hard copy document might be authenticated through the testimony of the document's author or the testimony of a person who saw the author sign the document. For electronic documents, the evidence required is less clear, and one requirement may be that the device used to produce the document was reliable. Therein lies the confusion. Is evidence required that shows the device was working reliably such that an accurate record was produced, or is more or less evidence required?

[6.2.1.3] For electronic evidence, it is important to demonstrate the provenance of the evidence and that the evidence has not been changed. This can be particularly difficult unless a forensic acquisition of the evidence has been made: see section 5.2 for a further discussion on this point.

[6.2.1.4] Authenticity may be provided through either testimonial or circumstantial evidence, or through a combination of both. In some instances, the authenticity of electronic evidence may be admitted by the parties, but the scope of the admission should be well understood, because an admission as to authenticity should not constitute an admission of the trust of the content of the electronic evidence. In the absence of testimonial evidence from the person who created the electronic evidence, or an admission by the parties as to authenticity, then circumstantial evidence of authenticity should be required. The party who challenges the authenticity or reliability of electronic evidence, by arguing it has been altered or tampered with, must provide evidence to support that challenge. Tampering goes to weight, not admissibility.

[6.2.1.5] For a document to fall within the Business Records Exception, pursuant to *Uniform Evidence Acts*, s 69, it must be satisfy the criteria that (a) it was a record created in the ordinary course of business and (b) that the person through whom the document is tendered

[758] *National Australia Bank Ltd v Rusu* (1999) 47 NSWLR 309, [17] (Bryson J).

has some personal knowledge of the record. The records must record the business activities and does not include the product of the business.[759] The person through whom the record is tendered must provide evidence that the document in question does form part of the records of the business,[760] notwithstanding that a reasonable inference could be drawn.[761]

[6.2.1.6] Where a business record also contains opinion evidence the representations contained in the document must also satisfy the requirements of *Uniform Evidence Acts* ss 78 or 79, for it to be admissible.[762] In any event, the opinion of the expert must have qualifications in compliance with the Expert Witness Code of Conduct.[763] Evidence can also be substantially outweighed by the danger that the evidence might be unfairly prejudicial to a party and might be misleading.[764] Lay opinion evidence may also be accepted pursuant to *Uniform Evidence Acts* s 78, if the document is admitted under the Business Records Exception. The opinion must be based on what the person 'saw, heard or otherwise perceived about a matter or event'[765] and must be 'necessary to obtain an adequate account or understanding of the person's perception'[766] of the matter or event.[767]

6.3 The Requirement to Authenticate in Other Jurisdictions

[6.3.1.1] In England and Wales, the judge has an explicit general power to exclude evidence when managing a case.[768] In order to call evidence about the provenance of the document in question, the creator of the evidence should be called to give evidence, that is the author of the document, or from the person who seized the computer who can testify as to the location at which the computer was seized, in whose possession the computer was at the time of seizure and the method used to obtain the electronic evidence. In the vast majority of cases,

[759] *Roach v Pages (No 15)* [2003] NSWSC 939 (20 October 2003).
[760] *Reidy v Elcheikh* [2006] FMCA 130 (24 March 2006), where a photocopy of a letter annexed to an affidavit did not include evidence that the letter formed part of the business records of the firm which wrote the letter.
[761] *Ringrow Pty Ltd v BP Australia Ltd* (2003) 130 FCR 569, [10]–[12].
[762] Refer *Tyneside Property Management Pty Ltd v Hammersmith Management Pty Ltd* [2011] NSWSC 395 (17 February 2011). As to the requirement that both the business record exception and the opinion exception be satisfied, see, in particular *R v Whyte* [2006] NSWCCA 75; and In the matter of *Enviro Energy Australia Pty Ltd (in liquidation)* [2010] NSW SC 1217 (23 September 2010), [7]; contra *ASIC v Rich* (2005) 216 ALR 320, [212-216].
[763] *Enviro Energy Australia Pty Ltd (in liquidation)* [2010] NSWSC 1217 (23 September 2010).
[764] Ibid [8].
[765] *Uniform Evidence Acts* s 78(a).
[766] *Uniform Evidence Acts* s 78(b).
[767] In *Lithgow City Council v Jackson* (2011) 244 CLR 352, the High Court confirmed that *Uniform Evidence Acts* s 78 codified the common law position on lay opinion evidence, especially as it relates to what the person perceived.
[768] *Civil Procedures Rules* (Eng), r 32.1.

it is rarely necessary to call an expert.[769]

[6.3.1.2] In the United States of America, the requirement to authenticate is governed by the *Federal Rules of Evidence* (USA), r 901, which provides that 'to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is'.[770] Authentication is a condition precedent to admitting evidence,[771] and may not be admitted into evidence unless it is shown to be genuine. Although the bar for authentication of evidence in the United States of America is not particularly high,[772] the requirement is satisfied if sufficient proof has been introduced so that a reasonable juror could find in favour of authenticity or identification.[773] Generally, however, the court has a broad authority to determine admissibility.[774] *Federal Rules of Evidence* (USA) r 901 provides several examples of proper authentication techniques in different contexts and these are 'not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law'.[775] A document can be authenticated by 'distinctive characteristics of the document itself, such as its '[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances'.[776] Although *Federal Rules of Evidence* (USA) r 901(a) addresses the requirement of authenticating electronically stored evidence, it is silent on how to do so. It does, however, provide examples of how authentication can be achieved. These examples include authentication through process or system which requires evidence describing the process or system used to produce a result and showing that the process or system produces an accurate result.[777]

[6.3.1.3] In Canada, the *Uniform Electronic Evidence Act* (Can) s 4(1) provides that

[769] *R v Shephard* [1993] AC 380.
[770] *Federal Rules of Evidence* (USA), r 901(a).
[771] *United States v Vayner*, F.3d, 2014 WL 4942227 (2d Cir. Oct. 3, 2014), quoting *United States v Sliker*, 751 F.2d 477,499 (2d Cir. 1948) at 497; see also *United States v Maldonado-Rivera*, 922 F.2d 934, 957 (2d Cir. 1990).
[772] *United States v Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007).
[773] *United States v Pluta*, 176 F.3d 43, 49 (2d Cir. 1999).
[774] In *United States v Sanders*, (1984) 749 F.2d 195, 197 (5th Cir. 1984).
[775] Fed. R. Evid. 901 advisory committee's note (Note to Subdivision (b)).
[776] *United States v Maldonado-Rivera*, 922 F.2d 934, 957 (2d Cir. 1990) (alteration in original) (quoting Fed. R. Evid. 901(b)(4) (pre at 2011 amendments
488 (contents of alleged bank records, in conjunction with their seizure at purported bank office, provided sufficient proof of their connection to allegedly sham bank).
[777] Ibid [37].

where the best evidence rule is applicable in respect of an electronic record, it is 'satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored'. The commentary to *Uniform Electronic Evidence Act* (Can) s 4 (1) explains that the purpose of the best evidence rule is to help ensure the integrity of the record, since alterations are more likely to be detectable on the original. The *Uniform Electronic Evidence Act* (Can) provides a test for the integrity of the record, which is the evidence of the reliability of the system that produced the record. The commentary to the Act states out that it will often be impossible to provide direct evidence of the integrity of the individual record to be admitted and system reliability is a substitute for record reliability. *Uniform Electronic Evidence Act* (Can) s 5 goes on to confirm that in absence of evidence to the contrary, 'the integrity of the electronic records system in which an electronic record is recorded or stored is presumed [in any legal proceeding]'. The commentary points out that this section is not intended to provide grounds for frivolous or expensive attacks on otherwise acceptable records, however, it leaves open the question of the integrity of the records system in which the evidence was created and stored. Further, s5(c) creates a presumption of reliability for business records. *Uniform Electronic Evidence Act* (Can) s 6 allows the court to consider any standards used in the storage of records.

6.4 The Reliability of Computer Systems

[6.4.1.1] With evidence produced by devices or systems, it appears the court must be satisfied, at least on the balance of probabilities in civil matters, of the accuracy of the technique used and the application of it.[778]

[6.4.1.2] Reliability of machines and devices is one issue, reliability of evidence created as part of a computer system, is another. This leads to the question as to whether the presumptions in *Uniform Evidence Acts* ss 146 and 147 can continue to apply to computer generated evidence. This was a key question considered by the ALRC and various submissions were put forward both for and against a more stringent test of reliability.

[6.4.1.3] Devices such as traffic lights, watches and speedometers have been presumed to work properly,[779] however with computers and computer-like devices, they are arguably

[778] Queensland Law Reform Commission, *The Receipt of Evidence by Queensland Courts: Electronic Records*, QLRC WP 52, August 1998, 8-9

[779] Mason, 'Electronic Evidence', above n 178 [5.02] citing *Tingle Jacobs & Co v Kennedy* [1964] 1 All ER 888.

more unreliable due to problems with software, including 'bugs'. [780] Mason[781] points out that whenever software is amended, the risk of defects increases and it is generally not until software is used in the 'real world' that defects are identified. Further, software is subject to vulnerabilities which means hackers and professional thieves can exploit such vulnerabilities, and often these activities can go undetected.[782] Mason[783] concludes that the presumption of reliability, especially for software, is fraught with problems and the reality is that the party contesting the presumption will rarely be in a position to offer substantial evidence to substantiate any challenge because the party facing the challenge will generally be in full control of the computer or computer systems that are the subject of the challenge.[784]

[6.4.1.4] Not only are changes in software problematic, it is the dynamic nature of computer-generated evidence itself that may cause issues. For example, the software application that displays a document, albeit working correctly, may change the metadata of the file, but not necessarily change the content itself. The type of device upon which the data are stored may affect the evidence, for example, the differences between a mainframe computer and PC, and information stored on an organisation's network and in the Cloud.[785]

6.5 Case Law on Authentication of Documentary Evidence in Australia

[6.5.1.1] In Australia, a few seminal cases discuss what is required to authenticate documents, and these are first examined, before looking at whether the law can be applied to the authentication of electronic documents.

[6.5.1.2] In *National Australia Bank Ltd v Rusu*[786] (*NAB v Rusu*) Bryson J carefully considered the law around the authentication of documents. In that case, the plaintiff bank, ('NAB') claimed that Ms Rusu stole a large sum of money from it with the assistance of another person, Mr Mato. NAB alleged that after stealing the money, Rusu and Mato had available to them a significant amount of funds compared with their previous resources. The NAB sought to recover the money allegedly stolen, assert charges and obtain tracing orders over their assets.

[780] Ibid [5.07].
[781] Ibid.
[782] Ibid [5.13] to [5.17].
[783] Ibid.
[784] Ibid [5.37].
[785] Lee Andrew Bygrave, *The Meaning of 'Data' and Similar Concepts - An Issue of Growing Legal Importance*, In Cecilia Magnusson Sjöberg & Peter Wahlgren (ed.) Festskrift till Peter Seipel (Norstedts Juridik AB 2006) 117 – 126.
[786] (1999) 47 NSWLR 309.

Counsel for NAB tendered two pages of what appeared to be a transaction history inquiry in relation to an account identified by number. However, nothing on the face of these pages identified the bank or the customer. There was evidence that the two pages were in a bundle of documents produced by Advance Bank in response to a subpoena that specified bank records for a different period, and to the effect that Advance Bank's customer was Mr Mato, whose full name was Peter Francis Mato. A solicitor for NAB made an affidavit attaching a schedule of payments, alleging that Mr Mato had paid a substantial sum of money into the Advance Bank account on the day after the alleged theft.

[6.5.1.3] In *NAB v Rusu*, Bryson J rejected tender of the two pages that purported to be part of the bank statement, and His Honour carefully distinguished between the authentication of documents, relevance, the procedure for proving the contents of documents and admissibility of representations in documents as business records notwithstanding the Hearsay Rule. Bryson J held it was necessary to establish by evidence, other than the documents themselves, that the pages were a bank statement, which comprised a statement of Advance Bank and that the account to which they referred was an account of Mr Mato. His Honour rejected the idea that under the *Evidence Act 1995* (NSW), the authenticity of documents tendered in evidence could be determined simply on the basis of the form and content of the document or on that basis taken with information about the source from which the document was produced, showing that it was produced on subpoena and by whom.

[6.5.1.4] Bryson J analysed the Australian Law Reform Commission's *Interim Report on Evidence,*[787] and noted that the Commission had addressed *Evidence Act 1929* (SA) s 45b, under which no authentication was initially required and it was enough that the document was apparently genuine. His Honour said: 'it does not seem possible that, after addressing 45b, the Law Reform Commission could have contemplated adoption of its principles without explicitly indicating that it was recommending this large change'.[788] Further, His Honour was of the view that there were some indications in the *Evidence Act 1995* (NSW) that were inconsistent with a wide general presumption of authenticity. In particular, Bryson J referred[789] to *Evidence Act 1995* (NSW) s 152, which deals with authentication in the case of documents more than 20 years old produced from proper custody, and *Evidence Act 1995* (NSW) s

[787] Australian Law Reform Commission, *Evidence (Interim),* Report No 26 (1985).
[788] (1999) 47 NSWLR 309, [316].
[789] Ibid.

144(1)(b), which refers to 'a document the authority of which cannot reasonably be questioned'.

[6.5.1.5] Authenticity is to be distinguished from relevance, as noted by Bryson J in *NAB v Rusu.*[790] Documents would be relevant if they were shown to be authentic and it was the evidence of authenticity that was lacking in the case before him. His Honour referred[791] to *Evidence Act 1995* (NSW) s 58(1) which provides that if a question arises as to the relevance of a document or thing, the court may examine it and may draw any reasonable inference from it, including an inference as to its authenticity or identity. His Honour said that the question of authenticity is not a question as to the relevance of documents within *Evidence Act 1995* (NSW) s 58(1), which 'treats authenticity as part of the material on which relevance may be determined'. Bryson J noted[792] that while there was some evidence with respect to compliance with *Evidence Act 1995* (NSW) s 69, that evidence was 'vehemently unsatisfactory' as a means of proof of the records of Advance Bank, and His Honour was not satisfied[793] on the balance of probabilities that the pages were what they were alleged to be.

[6.5.1.6] It has since been recognised that Bryson J's reasoning in *NAB v Rusu* showed that the Australian Law Reform Commission did not intend general abolition of the requirement to authenticate documentary evidence, and identifies indications in the *Evidence Act 1995* (NSW) that the authentication requirement has been generally preserved.[794] Specifically, on Bryson J's approach to *Evidence Act 1995* (NSW) s 69, it does not override the requirement to authenticate. The concepts are distinguished from one another in the *Evidence Act 1995* (NSW), which allocates different chapters to ways of adducing evidence (Chapter 2), admissibility (Chapter 3) and proof (Chapter 4), but the conceptual distinctions are sometimes overlooked in practice.[795]

[6.5.1.7] *NAB v Rusu* was cited with approval in subsequent cases,[796] however, Bryson

[790] Ibid [313].
[791] Ibid [313].
[792] Ibid [317].
[793] Ibid 318.
[794] *ASIC v Rich* (2005) 216 ALR 320, [104] (Austin J).
[795] Ibid.
[796] In *Daw v Toyworld (NSW) Pty Ltd* (2001) 21 NSWCCR 389, the appellant had brought proceedings for damages for a workplace injury. One of the grounds of appeal was that the trial judge had erred in placing reliance on a set of clinical notes of unknown origin. Heydon JA (with whom Priestley and Sheller JJA agreed) rejected this ground because it had not been shown that the trial judge placed reliance on this material, and no objection to its admissibility had been taken at the trial. His Honour added '.. if the document was of unknown

J's reasoning in *NAB v Rusu* was criticised by Stephen Odgers SC, in the fifth edition of *Uniform Evidence Law.*[797] Odgers, after quoting Bryson J's observation that the question of authenticity is not a question as to the relevance of documents within s 58(1), he inferred that on Bryson J's approach the court may not draw reasonable inferences from a document as to its authenticity, rather, he suggested that such view is inconsistent with the intention behind s 58(1) and its legislative history.

[6.5.1.8] In *Lee v Minister for Immigration & Multicultural & Indigenous Affairs,*[798] Madgwick J took up Odgers' criticism. In that case, the question before the court was whether an applicant for review of a decision by the Migration Review Tribunal had applied within time and that depended upon whether the Minister had discharged the onus of proving that notification of his decision had been sent by registered mail to the applicant at a certain time. Two pieces of evidence were relied upon by the judge at first instance. The first was contained in an affidavit about the Department's database, which contained information recorded by a named officer, representing that a notification letter had been sent to the applicant in Australia on a certain date by registered mail. The second piece of evidence was a note by an unnamed author scanned into the database on the following day, according to which an unnamed person at Australia Post had said that the letter of the previous day was in the Australia Post delivery centre. One of the arguments advanced by the applicant was that the note was inadmissible as a business record, having regard to *NAB v Rusu*. Hely J held that the note was admissible under s 69 notwithstanding that the person who made the note and the person in Australia Post who supplied the information were unknown. His Honour said that s 69(2)(b) 'applies as I am satisfied that the notation was made in the course of, and for the purposes of, the respondent's business on the basis of information directly supplied by a person from Australia Post who might reasonably be supposed to have had personal knowledge of a certain fact.[799] Madgwick J described *NAB v Rusu* as 'controversial NSW authority', citing the passage in the fifth edition

origin, it could have been objected to as unauthenticated and irrelevant. The *Evidence Act 1995* does not permit documents to authenticate themselves save in limited circumstances [citing *Rusu*]). See also, *Kingham v Sutton (No 3)* [2001] FCA 1117 (15 August 2001) [127] (Goldberg J) and *Citibank Ltd v Chiu Wah Liu* [2003] NSWSC 236 [3] (Hamilton J). In *Crime Commission (NSW) v Trinh* [2003] NSWSC 811 (5 September 2003) Hidden J at [14] drew attention to the distinction between authenticity of records and accuracy of records. His Honour had distinguished *Rusu*, while not disagreeing with it, on the ground that the argument before him, relating to some casino records, was concerned with their accuracy rather than authenticity.

[797] Stephen Odgers, *Uniform Evidence Law (*Thomson Reuters, Australia, 6th ed, 2004) 183.

[798] [2002] FCAFC 305 (4 October 2002).

[799] Ibid, [18].

of Odgers referred to above, and continued:

> In *Rusu*, his Honour may have meant no more than that there may be cases in which, as a matter of fact, no inference as to authenticity of a document may be properly drawn from the document itself. If he meant to say more than that, it is by no means clear to me that the way is open for a court to read some unexpressed limitation into a grant of power to courts: such grants are generally very liberally construed … Such an approach may be particularly apt where, as here, the provision aims at putting another nail in the coffin of unmeritorious technicality in litigation and s 135 provides ample safeguards against possible abuse of the section. [800]

[6.5.1.9] In *O'Meara v Dominican Fathers,*[801] the Court of Appeal of the Australian Capital Territory considered *NAB v Rusu*. There, the appellant sued the operators of a university residential college for personal injury when she fell off a balcony after drinking alcohol. A question on the appeal was whether a hospital report, supported by evidence by a pharmacologist, which showed a high blood alcohol concentration, should have been allowed into evidence. It was argued that the hospital report did not prove itself, and as there was no evidence of the nature of the tests that were performed, how they were performed or who supervised them, the report was not authenticated in the manner required by *NAB v Rusu* and should have been rejected. Gyles and Weinberg JJ held that in light of the evidence of the pharmacologist, the report had been properly received in evidence, relying specifically on s 146. However, on the general requirement of authentication they referred to *NAB v Rusu* and said:[802]

> In that case, his Honour appeared to hold that the fact that a bank had produced copy bank statements on subpoena did not prove that they were bank statements of the relevant account that was identified on them, and that further proof of authenticity was required. We have considerable doubt as to the applicability of that decision to the present circumstances. Admissibility of evidence is to be judged on the balance of probabilities (s 142), with the benefit of the inferences to which we have already referred (s 183), with the facilitating provisions of s 48 and (in the present case) s 146, dealing with evidence produced by processes, machines and other devices. *Rusu* may also be at odds with the thrust of the judgments in *Albrighton v Royal Prince Alfred Hospital*[803], per Hope JA at 547-550 and Hutley JA at 565-571, although the text of the legislation there in question differed from the Evidence Act. *Albrighton* does not seem to have been cited to Bryson J in *Rusu*.

[6.5.1.10] In *Albrighton v Royal Price Alfred Hospital*[804] there were issues about the admissibility of hospital records as business records, however, that there did not seem to have

[800] Ibid [25].
[801] [2003] ACTCA 24 (5 December 2003).
[802] [2003] ACTCA 24 (5 December 2003), [85].
[803] (1980) 2 NSWLR 542.
[804] Ibid.

been an issue about the authentication of the documents. Authenticating evidence was given by a hospital administrator. The issues in the Court of Appeal related to such questions as whether the authenticating evidence should have been taken in the absence of the jury, and whether it should have been rejected because it contained medical opinions expressed by persons who may have been unqualified, or because it contained unintelligible or ambiguous entries.

[6.5.1.11] The decision in *NAB v Rusu* was considered at length and approved in *ASIC v Rich*.[805] In that case, ASIC sought to tender 12 lever-arch folders, which were exhibits to an expert report which Austin J had earlier held to be inadmissible, in addition to a six-folder tender bundle. Many of the documents originated from the finance directory on One.Tel's server. ASIC relied on a description of One.Tel's computer system provided by One.Tel's senior database administrator. He said that One.Tel's accounting system contained all ledgers, and detailed financial data was summarised and then purged from the system during normal month-end processing. The senior database administrator explained how data could be accessed in the accounting system, by using a username and password recognised by the system. One.Tel used a separate disk drive on the file server to store administration and management files and the disk drive was referred to within the organisation as the 'I:/Drive' or the data drive. The files in the I:Drive were obtained under a search warrant and the files were extracted by a forensic technology expert. These files, once extracted, were made available to ASIC on a hard disk.

[6.5.1.12] The defendants contended that ASIC's provenance evidence failed to address a matter of fundamental importance in a case such as this, namely the authenticity of the documents. According to the defendants' submission, documents do not prove themselves, and need to be authenticated, in effect as a condition precedent to relevance and to admissibility under the Business Records Exception. Reference was made to the statement of Bryson J in *NAB v Rusu*.[806] ASIC claimed that its provenance evidence, which identified the source of the documents in the 'I:/Drive' or elsewhere, when considered with what is on the face of the documents themselves, was sufficient foundation for the tender of the documents, which can then be allowed to speak for themselves. It challenged *NAB v Rusu* to the extent that the case

[805] (2005) 216 ALR 320.
[806] (1999) 47 NSWLR 309.

would impose any higher requirement of authentication. ASIC invited the court to order that any one or more of the provisions of Part 2.2 or Part 3.2 of the *Evidence Act 1995 (NSW)* do not apply in relation to evidence going to the authenticity of the documents tendered, on the ground that this 'matter' is not genuinely in dispute. However, Austin J,[807] considered that the defendants had an arguable case in the difficult area of authentication of documents. Austin J examined the 1999 decision in *Rusu*. Austin J stated that:[808]

> In the case of a business record, its authenticity may be proved, at the simplest, by the evidence of a person who satisfies two conditions: namely, first, that he or she participates in the conduct of the business; and secondly, that he or she compiled the document, or found it among the records of the business, or can recognise it as one of the records of the business.

[6.5.1.13] In referring to Bryson J's decision in *NAB v Rusu*, Austin J said that his Honour did not have in mind proving the authenticity of the business record 'by the evidence of a person unconnected with the business who has found the document among the records of the business or can recognise it as a business record.'[809] After reviewing the authorities, Austin J summarised that[810] the suggestion that *NAB v Rusu* may be at odds with *Albrighton* relates to Bryson J's unwillingness, in the case before him, to draw inferences as to authenticity from the face of the document and circumstances of its production. His Honour considered that[811] the point made about *NAB v Rusu* in *O'Meara* is essentially the same as the criticism made by Madgwick J in *Lee* and by Odgers, namely that authentication may be established by inferences, including inferences from the form and contents of the document tendered. Austin J considered that[812] it would be absurd, according to Bryson J in *NAB v Rusu*, for the law to dispense on a general basis with the need to prove the authenticity of a document:[813]

> … for that would 'put the court entirely in the hands of whatever a document which a party chose to tender purported to be, subject to whatever opportunity another party had of overcoming its apparent effect'. On the other hand, it is important not to set the bar too high for the authentication of documents, because if too much is demanded, the authentication requirement will fight against the policy underlying the business records provisions which, as Hope JA remarked in *Albrighton* (at 548), is 'of great importance in the search for truth'. That policy recognises that any significant organisation depends for its efficiency upon the keeping of proper records, to be used and relied upon in the everyday carrying on of the activities of the business and therefore likely to be accurate, and 'likely to be a far more reliable source of truth than memory' (*Albrighton*, at 548-549 per Hope JA; see also

[807] Ibid [94].
[808] (2005) 216 ALR 320, [99].
[809] Ibid.
[810] Ibid [114].
[811] Ibid [115].
[812] Ibid [116].
[813] (1980) 2 NSWLR 542, 315.

> Australian Law Reform Commission, *Interim Report on Evidence* (Report No 26, vol 1), at [709]). It is reflected in the terms of s 69, which makes hearsay representations in business records admissible without requiring evidence from their authors.

[6.5.1.14] There is a distinction between authentication and the weight or probative value of documents. In *NAB v Rusu*, Bryson J did not deny that inferences may be drawn from the document itself, relevant to the question of authenticity. Austin J[814] noted that apart from s 58(1), there is express statutory authority to do so in s 183, when a question arises in regards to the applicability of a provision of the Evidence Act. However, Austin J considered that *Rusu* insists on the need for authenticity to be established, and asserts that authentication cannot be achieved *solely* by drawing inferences from the face of the document where there is no other evidence to indicate provenance. In His Honour's opinion, the other cases do not deny these propositions.[815]

[6.5.1.15] Austin J concluded that authentication is about showing that the document is what it is claimed to be, not about assessing the document. At the point of the adducing of the evidence, authentication is based on whether the document proves what the tendering party claims it proves. This means that a tendering party must show something more than the mere tender of the document itself where the tender is contested. If the tendering party adduces provenance evidence then the court can conclude on the balance of probabilities, pursuant to *Evidence Act 1995* (NSW) s 142, that the document had been adequately authenticated. That evidence does not show who created the document, how the document was used within the organisation, or even whether it is the only version or might have been a draft.

[6.5.1.16] In *Matthews v SPI Electricity Pty Ltd (Ruling No 35)*,[816] relevance was decided upon by relying on Austin J's reasoning in *ASIC v Rich* (following the earlier decision in *NAB v Rusu*), in not requiring evidence from the creator of a document to prove its authenticity, but requiring something in addition to the mere tender of the document itself to establish its provenance.

[6.5.1.17] Once the document is in evidence, it is open to the other party to give evidence

[814] (2005) 216 ALR 320, [117].
[815] Ibid.
[816] [2014] VSC 59 (27 February 2014) [28].

to contradict, undermine or explain the document[817]. Thus, it is open to the other party to challenge the accuracy of the document or to seek to show that was only a draft and was never treated as final or relied on. The burden of proof is on the other party once the authenticity of the document has been established, that is, once it has been shown to the requisite evidentiary standard that the document is what it purports to be.

6.6 Authentication of Electronic Documents in Australia

[6.6.1.1] The authorities set out in [6.5.1.1] to [6.5.1.17] above, make it clear that documents cannot authenticate themselves, and that there must be some form of extrinsic evidence to authenticate the documents. How do these rules apply to electronic documents?

[6.6.1.2] In *ASIC v Rich*, documents from a file server had been tendered as evidence, and their provenance was questioned. After consideration of the authorities and of the evidence before him, Austin J, in *ASIC v Rich* concluded that there were sufficient grounds to authenticate each category of documents, which were originated on servers at One.Tel. In arguing against authentication, the defendants had made two general submissions about authentication, which his Honour considered. First, the defendants submitted that the fundamental problem with all categories of documents was that ASIC had brought forward no one who was involved in the creation or keeping of the documents who could verify that they were final and operative documents as they existed at any particular point of time, as opposed to merely some drafts or scenarios on variable assumptions. His Honour considered that the requirement to authenticate a document is not a requirement to produce a witness involved in the creation or keeping of the document. Other means of authentication may suffice. With respect, no evidence was tendered regarding the software used, and the computer system in which it was kept, and integrity of that system. With respect, while his Honour made the correct conclusion regarding means of authentication, without evidence as to the integrity of the record keeping system, how can the court be satisfied of the means of authentication used?

[6.6.1.3] Secondly, the defendants emphasised the importance of the documents to ASIC's case and the fact that this is a civil penalty proceeding in which allegations are being made of serious misconduct, giving rise to the considerations enunciated by the High Court in

[817] Refer *Albrighton* (1980) 2 NSWLR 542, 570 [103] (Hutley JA); Australian Law Reform Commission, Evidence (Interim), Report No 26 (1985).

Briginshaw v Briginshaw.[818] However, his Honour did not regard this submission affected the question as to whether documents have been adequately authenticated. His Honour considered[819] that documents can be authenticated by such evidence about their nature and provenance as will give rise to the inference that they are what ASIC claims they are. Once they are adduced in evidence, it is open to the defendants to show that they have no probative value, for example by establishing that they were drafts not acted upon or that they were based on assumptions or scenarios not widely held within the company. Austin J tempered this by saying that the law does not overload the authenticity requirement by including within it an obligation for the tendering party to rebut all such possibilities, and issues going to the ultimate probative value of the documents could not be assessed at that stage as they did not bear on authentication. Austin J held that it would be setting the standard of authentication at too high a level to require ASIC to show, in the case of each document, that it is unique and not simply one of several versions. With respect, the issues regarding authentication of electronic evidence is about the system in which the evidence, whether they be drafts or final versions, are what need to be considered by the court.

[6.6.1.4] In *ASIC v Rich,* Austin J held that the question whether a particular document is one of several versions should be addressed in light of all the evidence, including such evidence as the defendants may choose to adduce. In that case, the documents in question were trial balances and were all headed 'trial balances' and the end-of-month dates were specified. They were located in the finance directory of the I:/Drive and their file paths indicate that they were trial balance or monthly balance sheet documents. His Honour considered that the fact that no trial balances were tendered for July, August and October 2000 did not bear on the authenticity of the documents. His Honour stated that the fact that a trial balance which is really for the month of April 2000 was incorrectly labelled 31 March 2000 did not prevent ASIC from authenticating the document, and was a matter to be decided once all the evidence had been adduced. The defendants set out a table of the trial balances, comparing asserted dates with dates 'modified', for documents where the document properties were available. The 'modified' dates were later than the asserted dates and the defendants submitted that the court could not confidently draw an inference that the document in its tendered form was available within One.Tel at any particular time. In some cases the 'modified' date was well before the

[818] (1938) 60 CLR 336.
[819] (2005) 216 ALR 320, [131].

appointment of voluntary administrators and in other cases the modified date was at a crucial time, but His Honour said these were matters going to probative value rather authentication.

[6.6.1.5] There were also management accounts, all headed as such for specified months. The documents, on their face, purported to be either profit and loss statements or statements of operating expenses. Some had footers indicating their character as management accounts and were located in the finance directory of the I:/Drive, the file paths of which also indicated their character as management accounts. His Honour made reference to the 'modified' dates being later than the asserted dates are anomalies which, if they are not explained by other evidence, will affect and possibly destroy the probative value of the documents in question, however, do not go to the authenticity of the documents.[820] With the greatest of respect to his Honour, it is this metadata within documents that can point to the integrity of documents produced, however, without reverting back to the original software that generated the reports in question, how can such reports be authenticated and relied upon? Most financial systems are contained within specially designed financial management software and reports, usually in a spreadsheet format, are exported from the financial management software. There does not appear to have been any evidence about the financial management software, how the reports were generated, or that the information that had been printed off was accurate. While the court, with respect, correctly stated that accuracy goes to probative value and that it is up to the other party to challenge the evidence, there does not appear to have been a challenge about the systems used to record, store and calculate financial reports of the company.

[6.6.1.6] Austin J referred to the Australian Law Reform Commission's observations about the analogous question of admissibility of hearsay representations in business records, in its *Interim Report*,[821] 'to the effect that errors can occur in written records but on the whole, they are more reliable than memory and the correct approach is to leave it to the party against whom the evidence is led to challenge it'.[822] *ASIC v Rich* was applied in *Australian Competition and Consumer Commission v Allphones Retail Ply Ltd* (No 4).[823] While this concept is, with respect, correct, again it fails to consider whether the evidence itself is authenticate, and is applying an old rule to new types of evidence.

[820] Ibid [140].
[821] Australian Law Reform Commission, *Evidence (Interim)*, Report No 26 (1985), vol 1, [705].
[822] Ibid.
[823] (2011) 280 ALR 97.

[6.6.1.7] With respect, it is true, that generally, business records should be accurate records which are indeed more reliable than memory. However, business records in electronic form are subject to manipulation from any number of sources and it is important to first ascertain that the record keeping system had a reasonable level of security around it. In *Australian Competition and Consumer Commission v Air New Zealand Limited (No 1),*[824] the court stated that if there is an issue regarding the authenticity of a document, it may still be admissible if it is relevant or arguably so. This is so as long as there is material from which its authenticity may reasonably be inferred. That material will include what may reasonably be inferred from the document itself. The process of determining whether or not documents are relevant, is integral to the discovery process, and technology, which is able to assist lawyers to review documents in their native, electronic format, is best placed to assist in a review for relevance.

[6.6.1.8] Evidence about the system, its integrity, and how reports were generated should have been, with respect, tendered and the witnesses should have, again with respect, given evidence as to the systems operation and reasonable level of security. With respect, an argument about provenance cannot be correct posed and answered without such evidence.

6.7 Authentication of Electronic Documents in England & Wales

[6.7.1.1] In England and Wales, evidence is governed by the *Civil Evidence Act 1995* for civil matters and the *Criminal Justice Act 1988* for criminal matters. Evidence is admissible as long as it is relevant to an issue in dispute, subject to a number of exceptions, such as the Hearsay Rule. The Business Records Exception to the Hearsay Rule applies in England and Wales. At common law, the best evidence rule applies, but this has been modified by the *Civil Evidence Act 1995* (Eng) and the *Criminal Justice Act 1988* (Eng).

[6.7.1.2] The authenticity of electronic data in legal proceedings has been considered on a case by case basis.[825] In *R v Cochrane,*[826] McCowan LJ, Waterhouse and Brooke JJ said that it was necessary for appropriate authoritative evidence to be called to describe the function and operation of a mainframe computer.

[824] (2012) 301 ALR 326.
[825] Mason, above n 178 [4.22].
[826] [1993] Crim LR 48 (CA).

[6.7.1.3] Documents in electronic format can be forged, as easily as documents in paper format. Email is one example of electronic documents that can be forged, however, this does not mean that every email needs to undergo an extensive authentication process to prove it is not a forgery. The authenticity of a document in electronic format can be tested in other ways.[827] In *R v Boulkhrif*,[828] the defence objected to the reliability and accuracy of bank transfers recorded on computer print-outs, which were initials by a bank clerk. The Court of Appeal indicated that while the initials provided evidence the transfers were authorised, they did not prove the authenticity of the documents. In comparison, in *R v Mawji (Rizwan)*,[829] evidence of a threat to kill included an email sent to the victim, which included the words 'I'm going to kill you'. The Court of Appeal rejected submissions that it was necessary to authenticate the email by showing the audit trail of where the email originated, as there was sufficient evidence showing the email was written and sent by the appellant. The court said that the content of the email demonstrated its authenticity on the face of the totality of the evidence. If the email had been fabricated, the Court asked why somebody would go to the length of forging the content of an email that was so obviously linked to the other evidence produced at the trial.

[6.7.1.4] Analysis of the metadata of an email showing where an email originated may be relevant to produce at the hearing. The email header can prove that the email was sent and received and show it was not a forgery. In *Greene v Associated Newspapers*,[830] emails were alleged to have been exchanged between Peter Forster and Martha Greene, a close friend of Cherie Blaire, the wife of the then Prime Minister of Britain. Ms Greene denied sending the emails to Peter Foster and claimed they were forgeries. An electronic evidence specialist examined Ms Green's computer and could find no trace of the emails. Another electronic evidence specialist examined three emails on a laptop owned by Mr Foster at his home in Australia and was able to complete a 'trace route' on the 'IP address headers'. The evidence was held to be sufficient to indicate that the emails were sent from a server in the Greater London area, and the mail servers in the email header were actual servers and the times recorded by the email header indicated that the times received were accurate. An email address header from the sender cannot be changed, although the sender of the email could have been

[827] Mason, above n 178 [137].
[828] [1999] Crim LR 73 (CA).
[829] [2003] EWCA Crim 3067, [2003] All ER (D) 285 (Oct).
[830] [2005] QB 972.

another person who had access to the owner's computer. When the email header was examined, it was found that it showed that from the point of departure to the addressee's inbox the emails had not been interfered with. Although the text of an email can be altered upon forwarding or sending the email to oneself or a third party, the original header would reflect this change, and there was no such indication in the header information of the emails in question. The Court of Appeal agreed with the trial judge that there was no clear 'knock-out' evidence to show the email was a forgery. Use of IP addresses within emails is useful, however, it cannot identify the person who drafted the email, but can only identify the person 'who has the contract with their ISP to have internet access'.[831] Authenticating pages from the Internet can be difficult because they alter frequently.[832]

[6.7.1.5] Circumstantial evidence can be used to authenticate an electronic document and such circumstantial evidence includes a range of factors including, but not limited to, appearance and the contents of the document, the subject matter, witness testimony, and any distinctive features that indicate a nexus.[833]

[6.7.1.6] Mason[834] summarises the position vis-à-vis authentication of electronic evidence, not only in England & Wales, but elsewhere, in five simple steps:

> (a) The data (both the content and associated metadata) that a party rely upon have not changed (or if the data have changed, there is an accurate and reliable method of recording the changes, including the reasons for any such changes) from the moment they were created to the moment they were submitted as evidence.
> (b) As a corollary to (a) above, it is necessary to demonstrate a continuity of the data not being altered between the moment the data were obtained for legal purposes and their submission as an exhibit.
> (c) As a corollary to (b) above, it should be possible to test any techniques that were used to obtain and process the data.
> (d) The data can be proven to be from the purported source.
> (e) The technical and organisational evidence demonstrates the integrity of the data is trustworthy, and is therefore considered to be reliable.[835]

6.8 Authentication of Electronic Documents in the USA

[6.8.1.1] In the United States of America, *Federal Rules of Evidence* (USA) r 901(b)(7)

[831] *Media CAT Ltd v Adams* [2011] FSR 28, [28] (Birss QCJ).
[832] *R v Skinner* [2005] EWCA Crim 1439.
[833] Mason, above n 178 [4.27].
[834] Mason, above n 178.
[835] Ibid Imwinkelried
.

permits authentication by public records or reports, including data stored in computers. Under this rule, there is no need to show that the computer system producing the public records was reliable or the records accurate.[836] In contrast, *Federal Rules of Evidence* (USA) r 901(b)(9) was designed for situations in which the accuracy of a result is dependent upon a process or system which produces it.[837]

[6.8.1.2] Ten years ago, Professor Imwinkelried[838] perceived electronic records as a form of scientific evidence and discerned an eleven-step foundation for computer records:[839]

1. The business uses a computer;
2. The computer is reliable;
3. The business has developed a procedure for inserting data into the computer;
4. The procedure has built-in safeguards to ensure accuracy and identify errors;
5. The business keeps the computer in a good state of repair;
6. The witness had the computer readout certain data;
7. The witness used the proper procedures to obtain the readout;
8. The computer was in working order at the time the witness obtained the readout;
9. The witness recognizes the exhibit as the readout;
10. The witness explains how he or she recognizes the readout; and
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

[6.8.1.3] With respect, this statement while helpful at the time to make sense of electronic evidence, is still based on print outs from a computer, and makes no reference to the computer system itself and its integrity. Further, this statement is now quite outdated, and a better checklist for authentication is that set out by Mason[840] as per section [6.7.1.6] above.

[6.8.1.4] In the case of *Re: VeeVinhnee*[841] the court explored the evidentiary foundation for introducing electronic documents as evidence. This matter was an appeal reviewing whether a trial court was entitled to insist upon a complete foundation, even in the absence of an objection. In that case, there was a claim by American Express ('Amex') to have an amount of a secured debt discharged in a bankruptcy matter. The trial court required proof of the entitlement to relief requested by Amex, and Amex had an employee testify that he was the custodian of records for the monthly statements, that the entries thereon were made on or about the time of the transactions, that the records were kept in the regular course of business, and

[836] Ibid [52]-[53].
[837] Ibid [54]-[55].
[838] Edward J. Imwinkelreid, *Evidentiary Foundations* (LexisNexis, 6th ed., 2005) 58-59.
[839] Referred to and approved in *Re: VeeVinhnee,* 336 B.R. 437 (B.A.P, 9th Cir, 2005).
[840] Mason above n 178, [4.21].
[841] 336 B.R. 437 (B.A.P, 9th Cir, 2005).

that the regular practice was to retain records.[842] The witness also confirmed that the term 'duplicate copy' appeared on the exhibits because the records were maintained electronically. The court explained that the electronic nature of the records necessitated, in addition to the basic foundation for a business record, an additional authentication foundation regarding the computer and software utilised in order to assure the continuing accuracy of the records. On the basis that the witness knew little about the computer software or hardware, the court deferred ruling on the admission of electronic billing statements but offered Amex the opportunity to cure the foundational defect later. Despite a post-trial submission, the court refused to admit the electronic business records because it concluded that the defective evidentiary foundation was not cured by the supplemental materials. In particular, the evidence submitted did not establish the qualifications of the witness to testify and the court did not perceive testimony that the business conducts its operations in reliance upon the accuracy of the computer in the retention and retrieval of the information in question.[843]

[6.8.1.5] Amex appealed the judgment and argued that in relation to the admission of its electronic business records into evidence it was an abuse of discretion for a court to require that all elements of an evidentiary foundation to be established by testimony of a qualified witness. Amex contended that the court was required to fill the gap by taking judicial notice of the accuracy and reliability of the Amex computer systems.[844] The court noted that the basic elements for the introduction of business records under the Business Records Exception for records of regularly conducted activity all apply to records maintained electronically. Such records must be: (1) made at or near the time by, or from information transmitted by, a person with knowledge; (2) made pursuant to a regular practice of the business activity; (3) kept in the course of regularly conducted business activity; and (4) the source, method, or circumstances of preparation must not indicate lack of trustworthiness. These elements must either be established by the testimony of the custodian or other qualified witness or must meet prescribed certification requirements.

[6.8.1.6] Such records, however, will not be admitted unless the court is also persuaded by their proponent that they are authentic. With electronic records, the court said that the focus must be on the circumstances of the preservation of the record during the time it is in the file

[842] Ibid [4].
[843] Ibid [6].
[844] Ibid [8].

so as to assure that the document being proffered is the same as the document that originally was created. The court said that logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and separately, how access to the specific program is controlled, are questions to be addressed. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.

[6.8.1.7] Paul has criticised the authentication of electronic evidence as being largely a 'trivial showing',[845] and makes the point that 'having a witness look at the order of the words on the first page of a recently printed electronic file does not logically entitle that witness, or our culture either, to make any assumptions whatsoever about the integrity of the order of the words in the middle of the document on page 54'.[846] In order to avoid a trivial showing, Paul suggests that 'something along the lines of the chain of custody that is required for certain easily changed artefacts is required.[847]

[6.8.1.8] Authentication renders evidence admissible, leaving the issue of its ultimate reliability to the jury.[848] Therefore, once evidence has been adduced sufficient to show the evidence is what it purports to be, the opposing party 'remains free to challenge the reliability of the evidence, to minimize its importance, or to argue alternative interpretations of its meaning, but these and similar other challenges go to the weight of the evidence – not to its admissibility'.[849]

[6.8.1.9] By 2007, courts in the United States of America were recognising that electronic evidence created a unique set of issues. In the landmark judgment of Judge Grimm in *Lorraine v Markel*[850], there were significant admissibility problems with the evidence, in particular, none of the documents presented were authenticated by affidavit or otherwise. Most of the facts relevant to contract negotiations at issue were provided by counsel without supporting

[845] Paul, above n 25, [48].
[846] Ibid.
[847] Ibid.
[848] *United States v Tropeano*, 252 F.3d 653, 661 (2d Cir. 2001).
[849] *United States of America v Tin Yat Chin* 371 F.3d 31 (2d Cir. 2004).
[850] 241 F.R.D. 534 (D.Md. May 4, 2007).

affidavits or deposition testimony. The evidentiary problems with the email evidence submitted were considered substantial because they were not authenticated.[851] The court noted that whether electronically stored information (ESI) is admissible is determined by a collection of evidence rules. Failure to clear any of these hurdles means that evidence will not be admissible. The court confirmed that whenever ESI is offered as evidence, the certain evidence rules must be considered, namely (a) is the ESI relevant,[852] (b) if relevant, is it authentic,[853] (c) if the ESI is offered for its substantive truth, is it hearsay[854] and if so, is it covered by an applicable exception[855], (d) is the form of the ESI that is being offered as evidence of an original or duplicate[856] and (e) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice[857] such that it should be excluded despite its relevance.[858] In that case, the failure of counsel collectively to establish the authenticity of their exhibits, resolve potential hearsay issues, comply with the original writing rule and demonstrate the absence of unfair prejudice rendered their exhibits inadmissible, resulting in the dismissal without prejudice, of their cross motions for summary judgment.[859] Interestingly, the court looked at the need for authentication and said that an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are also many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output.[860] The court noted that when evaluating the reliability of computer-based evidence, factors that should be considered include the error rate in data inputting and the security of the systems. The degree of foundation required to authenticate computer-based evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routineness of the computer operation, and the ability to test and verify results of the computer processing.[861]

[6.8.1.10] According to Judge Grimm, a witness must provide factual specificity about the process by which electronic evidence is created, acquired, maintained, and preserved without

[851] Ibid [12].
[852] As determined by *Federal Rules of Evidence* (USA) r 401.
[853] As required by *Federal Rules of Evidence* (USA) r 901(a).
[854] As determined by *Federal Rules of Evidence* (USA) r 801.
[855] As per *Federal Rules of Evidence* (USA) rr 803, 804 and 807.
[856] As per *Federal Rules of Evidence* (USA) rr 1001-1008.
[857] Or one of the other factors identified by *Federal Rules of Evidence* (USA) r 403.
[858] *Lorraine v Markel* Ibid 241 F.R.D. 534 (D.Md. May 4, 2007), [15]–[16].
[859] Ibid [188].
[860] Ibid [35].
[861] Ibid [36].

alteration or change, or the process by which it is produced if the result of a system or process that does so, as opposed to boilerplate, conclusory statements that simply parrot the elements of the Business Records Exception, or public record exception.[862] In *Lorraine v Markel*, Judge Grimm referred to the authentication or identification by comparison by the trier of fact or expert witnesses with specimens which have been authenticated.[863] Documents, including emails and other electronic records, can be authenticated or identified by 'appearance, contents, substance, internal patterns, or with circumstances'.[864]

[6.8.1.11] Metadata can be used to authenticate evidence, and Judge Grimm confirmed that the *Federal Rule of Civil Procedure* (USA)[865] allows a party to discovery ESI and identify the forms in which it is produced. The party can request production of ESI in its 'native format' which includes the metadata for the electronic document. The metadata shows the date, time and identity of the creator of the electronic record, as well as changes made to it. Accordingly, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate an electronic document.[866]

[6.8.1.12] Judge Grimm recognised that authenticating electronically stored information presents a myriad of concerns because 'technology changes so rapidly' and is 'often new to many judges'.[867] Further, the 'complexity' or 'novelty' of electronically stored information, with its potential for manipulation, requires greater scrutiny of 'the foundational requirements' than letters or other paper records, to bolster reliability.[868]

[6.8.1.13] In the United States of America, when courts are considering whether the elements of the business record exception to the Hearsay Rule[869] are established, they do so concomitantly with authenticity.[870] Indeed, the courts have been willing to think 'outside the box' to recognise new methods of authentication, and a presumption of authenticity has been

[862] Ibid [42].
[863] As allowed by *Federal Rules of Evidence* (USA) r 901(b)(3).
[864] *Lorraine v Markel* Ibid 241 F.R.D. 534 (D.Md. May 4, 2007) [43]-[44].
[865] *Federal Rule of Civil Procedure* (USA) r 34.
[866] Ibid [48]-[50] in referring to *Federal Rule of Civil Procedure* (USA) r 901(b)(4).
[867] Ibid at 544.
[868] Ibid at 543-44, quoting Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence § 900.06[3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997).
[869] *Federal Rules of Evidence* (USA) r 803(6).
[870] *Federal Rules of Evidence* (USA) r 902(11)

acknowledged by the court.[871] The courts have considered circumstances where it is possible that third persons other than the sponsor of a website were responsible for the contents of the postings.[872] The foundational concerns encountered when authenticating website evidence similarly apply to text messages and instant messaging content. In particular, posts in chat rooms are often posted by third parties under screen names meaning it cannot be assumed that the content in chat rooms was posted with the knowledge or authority of the website host.[873]

> Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.[874]

[6.8.1.14] The court commented that there has been a wide disparity between the most lenient positions courts have adopted in accepting electronic records as authentic and the more demanding requirements for authentication that have been imposed.[875] In *State v Navjot Sandhu*,[876] a case that considered the authenticity of prints of mobile phone calls, the courts said that the 'definition of authenticity in respect of a physical document comprises such attributes as the state of being of the original, or more appropriately, of being faithful to an original, uncorrupted and perhaps, with a verified provenance (comprising the following attributes: unique, unambiguous, concise, respectable and comprehensible).'[877]

[6.8.1.15] A witness can testify that she received and printed emails on her computer in order to authenticate the email.[878] Emails obtained by a trained computer forensics expert can be used to authentic emails, as long as the chain of custody is preserved.[879] However, in order

[871] For example, in *Indianapolis Minority Contractors Ass'n* 1998 U.S. Dist. LEXIS 23349, the court held that documents provided during discovery by an opposing party are presumed to be authentic, shifting the burden to the producing party to demonstrate that the evidence they produced as not authentic, approved in *Lorraine v Markel* 241 F.R.D. 534, [68].
[872] Ibid [78].
[873] Ibid [81]-[82].
[874] Ibid [84] referencing Manual for complex litigation 11.447.
[875] Ibid [91]-[92].
[876] (2005) 11 SCC 600.
[877] Attributes suggested in Philip Turner, 'Digital provenance – interpretation, verification and corroboration' (2005) 2(1) *Digital Investigation: The International Journal of Digital Forensics & Incident Response* 45-49.
[878] *Kearley v Mississippi*, 843 So.2d 66 (Miss. Ct. App. 2002).
[879] *Kupper v State* 2004 WL 60768 (Tex. App. Jan. 14, 2004), where the court concluded that the computer forensic expert's testimony established that the appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances, authenticated the computer evidence.

to authenticate pages printed from social networking sites, a print will not necessary be enough, and evidence to show who created the page and was responsible for its content will be necessary.[880] Indeed, social networking sites are notoriously difficult to authenticate because 'a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate'.[881] Anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password. There is no law that prevents someone from establishing a fake account under another person's name, so long as the purpose for doing so is not to deceive others and gain some advantage.[882] Instant messages can be authenticated through a witness as long as the recipient identifies his or her 'distinctive characteristics.[883]

[6.8.1.16] Printouts from social networking sites can be admitted in certain circumstances where the creator provides testimony that the printout is what it purports to be, [884] the computer of the alleged creator of the profile is searched and the computer's internet history and hard drive is examined to determine if that computer was used to create the social networking profile[885] or other information may be obtained directly from the social networking that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it.[886]

---

[880] In *United States v Vayner*, F.3d, 2014 WL 4942227 (2d Cir. Oct. 3, 2014), the court held that the court below had abused its discretion in admitting the web page that had been printed off from a Russian social networking site, akin to Facebook, holding that the document had not been properly authenticated under *Federal Rules of Evidence* (US) r 901. The court held there was not a sufficient basis on which to conclude that the printout was what it claimed it to be, that is, Mr Zhyltsou's profile page; therefore, there was insufficient evidence to authenticate the page and permit its consideration by the jury. Although information about Mr Zhyltsou appeared on the web page: his name, photograph, and some details about his life consistent with a witness' testimony about him, there was no evidence that Zhyltsou himself had created the page or was responsible for its contents. Interestingly the court went on to say that 'Had the government sought to introduce, for instance, a flyer found on the street that contained Zhyltsou's Skype address and was purportedly written or authorized by him, the district court surely would have required some evidence that the flyer did, in fact, emanate from Zhyltsou. Otherwise, how could the statements in the flyer be attributed to him?'.

[881] *Griffin v State of Maryland* No. 74, Sept. Term, 2010, citing Petrashek, 93 Marq. L. Rev. at 1499 n 16.

[882] Compare *State v Bell* 2009 Ohio App. LEXIS 2112 (Ohio Ct. App. 2009) where defence counsel had expressly approved the admission of social networking emails and messages.

[883] *In the Interest of F.P.*, 878 A.2d 91 (Pa. Super. Ct. 2005)

[884] See, e.g., Katherine Minotti, Comment, The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession, 60 S. C. L. Rev. 1057 (2009).

[885] Referring to: Seth P. Berman, et al., Web 2.0: What's Evidence Between "Friends"?, Boston Bar J., Jan.– Feb. 2009, 5, 7.

[886] This method was apparently successfully employed to authenticate a MySpace site in *People v Clevenstine*, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009).

6.9 Authentication of Electronic Documents in Canada

[6.9.1.1] In Canada, *Uniform Electronic Evidence Act* (Can) s 3 provides that 'the person seeking to introduce an electronic record [in any legal proceeding] has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be'. Evidence as to system reliability cannot, of course, guarantee the integrity of the record, but it does go some way to supporting its integrity to a degree that the courts can admit the record, subject to an argument about its weight. The Canadian Act was enacted in 1998 and since then, commentators have questioned the effect of the provisions of that Act.

[6.9.1.2] Chasse suggests[887] that the authentication rule at times appears inadequate, because it cannot be established that an electronic record is the same as its first instantiation simply by looking at the record itself. Duranti, Rogers & Sheppard posit that the *Uniform Electronic Evidence Act* (Can) renders it necessary to refer to an unbroken line of traces left by all those who interacted with the record or to the legitimate custody of a professional who can account for them,[888] suggesting that the weight is on the integrity of the system, rather than the record. The authentication rule, at times, appears inadequate as originality cannot easily be established.

[6.9.1.3] The *Uniform Electronic Evidence Act* (Can) applies a presumption of integrity of the system to electronic records produced by a party. The commentary to the Act provides that a litigant's own records management system can qualify as a 'standard'.[889] However, Chasse[890] has questioned whether this goes far enough and asks whether it would be more accurate to refer to a formally accepted and implemented policy that contains practices and procedures. Further, relying on one's own system could lead to a 'pointless circularity'. In determining admissibility, it would remain up to the judge to decide which policy was

[887] Ken Chasse, *The Admissibility of Electronic Business Records*, (2011) 18:2 Canadian Journal of Law and Technology 105-191 at 111.

[888] Luciana Duranti, Corinne Rogers and Anthony Sheppard, 'Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later' (2010) 70 *Archivaria* 95, 98; see also Heather MacNeil, 'Providing Grounds for Trust: Developing Conceptual Requirements for the Long-term Preservation of Electronic Records,' (2000) 50 *Archivaria* 52–78; Luciana Duranti and Kenneth Thibodeau, 'The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES,'(2006) 6(1) *Archival Science* 13–68, <http://dx.doi.org/10.1007/s10502-006-9021-7> at 18 October 2009; Luciana Duranti, 'From Digital Diplomatics to Digital Records Forensics,' (2009) 68 *Archivaria* 39–66.

[889] *Uniform Electronic Evidence Act* (Can) s 6.

[890] Chasse, above n 512.

appropriate in the circumstances and whether the electronic record in question were created, maintained and preserved in accordance with the policy. Once electronic evidence is ruled admissible, then the trier of fact can consider it. The question of weight has been left open.

[6.9.1.4] In terms of general acceptance and implementation, the *Uniform Electronic Evidence Act* (Can) was a great success, and literally became uniform law across Canada, regulating the admissibility of electronic records offered into evidence in all criminal and most civil, quasi-criminal, and administrative proceedings.[891] Most legislatures, including the federal one, implemented the provisions of the *Uniform Electronic Evidence Act* (Can)[892], while four Canadian jurisdictions declined,[893] and two[894] enacted distinctive provisions that do not apply to criminal proceedings.

[6.9.1.5] Duranti, Rogers & Sheppard[895] suggest that the rules of admissibility that focus on authentication and the best evidence rule within the *Uniform Electronic Evidence Act* (Can) are closely tied to the computer technology that existed in the 1990s, and suggest that the Act 'does not provide any guidance with respect to issues of relevance or weight, and offers only cursory reference to other rules of law such as the hearsay rule'. Furthermore, it has also been suggested that the Act in its current form is 'subject to the criticism that it perpetuates the increasingly irrelevant best evidence rule, fails to address hearsay issues, and conflicts with existing statutory exceptions', and that:

> The most important failing of the Act, however, is its misleading treatment of electronic evidence as susceptible to governance by one set of brief rules that presupposes a fixed technology. While this approach might have been appropriate back in 1997–1998 when the Act was developed, the subsequent growth of digital technology has made it untenable. Digital technology raises the most profound challenges yet to the traditional evidentiary concepts of relevance, admissibility and weight, and puts into question the very idea of record as embedded in the admissibility rules of the law of evidence. In addition, the common understanding of relevance and weight is more open than ever to scrutiny in the digital world. When the Act was formulated, the profound impact of digital technology was not fully comprehended, and the Act suffers as a result.[896]

[891] Duranti, Rogers & Sheppard, above n 888, 102.

[892] Most legislatures, including the federal one, implemented the provisions of the *Uniform Electronic Evidence Act* (Can) by renumbering them and inserting them as amendments into their pre-existing evidence acts. Two legislatures (PEI and the Yukon Territory) enacted the Act as a distinct statute, physically separate in the statute books from their evidence acts. The act was further validated in common law, in *R. v Bishop* [2007] OJ No 3806 (QL) 75 WCB (2d) 258, [30] where the new rules were described as a 'mini-code', implying that, they were effective and prevailed over other provisions, a decision that would maximise their impact.

[893] British Columbia, New Brunswick, Newfoundland and Labrador, and Quebec.

[894] New Brunswick and Quebec.

[895] Duranti, Rogers & Sheppard, above n 888, 98; see also MacNeil, above n 888; see also Duranti & Thibodeau above n 888.

[896] Ibid.

[6.9.1.6] In addition to records stored on computer systems, are those records that have been seized. Duranti, Rogers & Sheppard are of the view that a limitation of the *Uniform Electronic Evidence Act* (Can), is that there is an absence of provisions related to the search and seizure of electronic records, and suggest that dramatic changes to the Act are required and that 'a new field of interdisciplinary knowledge needs to emerge that will provide the conceptual and methodological foundation for these changes'.[897] Legislation that is aimed at regulating the admission of electronic records into legislation must 'result from an integration of the knowledge and perspectives of legal and law enforcement professions, the records professions and the information technology profession'.[898] The commentators suggest that such an interdisciplinary approach will not only relieve inconsistencies in the interpretation of evidence but also help individuals and organisations understand how they can create, maintain and preserve electronic materials to ensure those materials are admissible if they are in court.[899]

[6.9.1.7] Whilst the *Uniform Electronic Evidence Act* (Can) is the leading generator for change in the law of evidence, in *R. v Ganes*,[900] it was held that electronic records were only admissible if they complied with the requirements of the common law, a judgment that would minimise the effect of the new requirements contained in *Uniform Electronic Evidence Act* (Can). Perhaps this decision confirms the limitations of the *Uniform Electronic Evidence Act* (Can), with its focus on authentication and the best evidence rule, but with little attention to the Hearsay Rule and Business Records Exception. Furthermore, the application of the Business Records Exception requires a clear concept of record and a clear methodology for identifying records in electronic systems.

[6.9.1.8] Chasse[901] argues that in the absence of fixed definitions of the phrases, the courts are allowed flexibility in applying them, however, argues that same flexibility leaves litigants and the business community uncertain as to what is required to prove business records as admissible and credible evidence.

[6.9.1.9] The need to maximise profits is assumed to be an unfailing and constant

[897] Ibid.
[898] Ibid.
[899] Ibid.
[900] [2005] S.J. No. 832 (Prov. Ct.), as discussed by Duranti, Rogers & Sheppard, above n 888., 103
[901] Chasse, above n 887, 126.

guarantee of a complete and accurate records and record-keeping system. However, Chasse[902] argues that in many situations now, incomplete and inaccurate records are necessary to maximise profits, or at least to minimise losses. For example, there are many more demands for the production of records by private litigants and government departments and regulatory agencies than was the case when the theory and the present law it supports, were created. Often it is more conducive to profit and to the avoidance of loss to destroy or 'lose' embarrassing and damaging records than to comply with the demands for their production. Regulatory authorities have much greater powers to force production of records and disclosure of information, and these are being used more frequently.[903]

[6.9.1.10] Chasse[904] argues that the test of admissibility should judge not the record alone, but the record system it comes from, since the Business Records Exception require that the record be judged, while the electronic record provisions require the record system to be judged. Therefore, Chasse argues they should be combined to create one test that judges the record system. That, Chasse suggests, can be accomplished by judicial interpretation that holds that evidence that satisfies the system integrity test of the electronic record provisions, satisfies the business record provisions, as well. Conversely, evidence that cannot satisfy the system integrity test should be held to be insufficient to satisfy the business record provisions. Chasse argues that the 'circumstances of the making of the record' test could be given that interpretation on the issue of admissibility and on the issue of weight in the business record provisions of the Evidence Acts. Similarly, he argues, the double 'usual and ordinary course of business' test should be given that interpretation of the issue of admissibility. For both issues, there is no effective way of judging the quality of an electronic record system, or of any electronic record, except by means of the system integrity test. [905]

[6.9.1.11] Gregory[906] has criticised Chasse's suggestion that a different rule for admissibility of electronic evidence be considered. Gregory argues that the law does not investigate the abilities of the humans who keep the records, therefore, why should it investigate the inner workings of a computer? Further, Gregory argues, the Business Records Exception arises from the presumption that businesses will create systems that increase the

[902] Ibid 118.
[903] Ibid.
[904] Ibid.
[905] Ibid.
[906] Ibid.

reliability of their records. This is the case as long as one is not referring to documents created when litigation is anticipated. Chasse[907] answered Gregory's critical question 'why should the law investigate the inner workings of a computer?' by stating that it has to. Chasse argues that the type of record system analysis required for judging the accuracy and reliability of a record from an electronic record system cannot be the same as that required for a traditional paper based system.[908] Further, Chasse argues that while technological changes do not always require changes to the law, in this case it is necessary. Traditional paper record systems gave rise to the legal concept of 'an original record', however, in electronic record systems there is no such 'original'. The printout that is often taken to court is produced at the end of the record system's functions and not at the beginning, that is, not at the time when the acts or event it records occurred and not by a person having 'direct personal knowledge'. [909]

[6.9.1.12] As early as 1979 in Canada, the courts have accepted that computer evidence is more complex than those of paper records, and recognised that the court should carefully scrutinise the foundation put before it to support a finding of reliability as a condition of admissibility.[910] The courts recognised that the nature and quality of the evidence put before the court has to reflect the facts of the complete records keeping process and in the case of computer records, the procedures and processes relating to the input of entries, storage of information and its retrieval and presentation.[911]

[6.9.1.13] Chasse points out that following this case, evidence is seldom presented as to the record keeping process. Witnesses who adduce such records are seldom cross-examined or otherwise challenged in argument. Therefore, he argues, the case law that should have been well developed post-1979 does not exist. This is not because the courts have chosen to ignore it, but probably because counsel appearing before the courts has ignored it.[912] System integrity should be limited to the types of defects within the preview of the best evidence rule (for which the system integrity test was created) and not those that the Hearsay Rule and its exceptions guard against as well. Such a system integrity test have the require foundation evidence for

[907] Ibid.
[908] Ibid.
[909] Ibid.
[910] *R. v McMullen* (1979) 100 DLR (3d) 671.
[911] Ibid per Mordan JA referring to *Transport Indemnity Co. v Seib* (1965), 132 N.W. 2d 871; *King v State ex rel. Murdock Acceptance Corp.* (1969), 222 So. 2d 393, and '*Note, Evidentiary Problems and Computer Records*', 5 Rut.J. Comp. L. 342 (1976), p. 355, et seq.
[912] Chasse, above n 512, 144.

admissibility that provides a comprehensive description of the working of that RIM system. Integrity has to be comprehensively applied.

6.10 Summary & Conclusion

[6.10.1.1] The analysis in this Chapter 6, shows that while there has been a comprehensive analysis of the law around authentication of documents, and the authentication of a document depends upon each case. First and foremost, the court is concerned with finding the truth. As Austin J noted in *ASIC v Rich*[913], agreeing with Bryson J in *NAB v Rusu*,[914] it is important that the court not set the bar too high for the authentication of documents, because if too much is demanded, 'the authentication requirement will fight against the policy underlying the business records provision; which is "of great importance in the search for truth"'.

[6.10.1.2] While the court recognises that the bar should not be set too high for the authentication of documents, has the bar been set too low for the authentication of electronic evidence? With the greatest of respect to the court, there does not seem to have been any analysis whatsoever of the electronic system in which the financial records of One.Tel were kept in *ASIC v Rich.*[915] It appears that while counsel did put before the court the fact that the dates modified in the electronic files, there did not appear to be any analysis of the system from which the reports in question were generated. Perhaps this was due to a lack of understanding about how electronic evidence is created, stored, and how documents are generated from electronic information.

[6.10.1.3] While the law in cases such as *NAB v Rusu* and *ASIC v Rich* is, with respect, well analysed and sound, neither of those cases dealt specifically with the anomalies in electronic evidence. In the United States of America, members of the judiciary, such as Judge Grimm, analysed electronically stored information ('ESI') and looked at ways in which such evidence can be authenticated, however, with respect, the cases in the United States of America state the problems with computerised evidence, but do not seem to offer any clear guidance on the initial hurdle in getting computer-generated evidence authenticated. With respect, it is Canada, and its provisions in the *Uniform Evidence Act* (Can), that recognises the true nature of electronic evidence. However, that Act was enacted in 1998 and since then, commentators

[913] (2005) 216 ALR 320.
[914] (1999) 47 NSWLR 309.
[915] (2005) 216 ALR 320.

have correctly, it is suggested, pointed out that the Act now requires updating to reflect the updates in technology during the last 17 years.

[6.10.1.4] It is suggested, with respect, that the *Uniform Electronic Evidence Act* (Can) goes a long way to setting out a more realistic process for authentication of electronic evidence, than any of the other evidence legislation. This is because that Act recognises that electronic evidence is unique, that it can be difficult to prove whether an original has been tampered with, and that in today's world, electronic evidence is created within the realm of a 'system'. The Act provides a presumption of integrity for a record keeping system in business, but allows this to be challenged.

[6.10.1.5] The questions following an analysis of the authentication of electronic evidence, are:

Question 6:
Do the presumptions in Uniform Evidence Acts ss 146 and 147 need modification to reflect the way in which electronic evidence is generated?

Question 7:
Are the current rules of authentication for documentary evidence, adequate to apply to electronic evidence?

7. CHAPTER 7 – SUMMARY & CONCLUSION

7.1 Summary of dissertation

[7.1.1.1] This research reveals that current rules of evidence embodied in the *Uniform Evidence Acts*, written substantially for documentary evidence, are applied to electronic documents inconsistently. It is clear that courts, and lawyers, lack a fundamental understanding of how electronic documents are created, stored and ultimately presented as evidence. It is very doubtful whether electronic documents are being properly authenticated before the courts, a process essential to the reception of all evidence as a condition of admissibility.

[7.1.1.2] The research has identified seven questions to be answered.

- Question 1: Are the laws recognising electronic signatures adequate for evidentiary purposes for documents?
- Question 2: Is the definition of 'document' in the *Uniform Evidence Acts* adequate for the purposes of electronic evidence and, in particular, does it appropriately identify the nature of electronic evidence in that it comprises both content and storage media?
- Question 3: Should the Business Records Exception, in its present form in the *Uniform Evidence Acts*, continue to apply to electronic evidence, or does it need modification?
- Question 4: Does the discovery process provide sufficient safeguards to ensure that the integrity of evidence remains intact?
- Question 5: For documents to which legal professional privilege applies, are there sufficient protection measures in place for retrieval of evidence on electronic media that contains privileged information?
- Question 6: Do the presumptions in *Uniform Evidence Acts* ss 146 and 147 need modification to reflect the way in which electronic evidence is generated?
- Question 7: Are the current rules of authentication for documentary evidence, adequate to apply to electronic evidence?

7.2 Electronic Signatures

Question 1:
Are the laws recognising electronic signatures adequate for evidentiary purposes for documents?

[7.2.1.1] Signatures are an effective way to show that a document is authentic, and that a party who signed the document intended to be bound upon it.[916] Until the rapid rise in the use of computers and consequent electronic transactions, the most common form of signature was a handwritten signature on a hard copy document.[917] This is notwithstanding that courts had recognised a wide range of marks as signatures.[918]

[7.2.1.2] Section 2.14 provides an overview of electronic signatures and demonstrates that there are various types of electronic signatures, including a name typed on an electronic document, a scanned manuscript signature, biometric measurements, a signature captured using a digital pen and accompanying software, and digital signatures.[919] Other forms of electronic signature include ways in which many people transact each day, such as the use of Personal Identification Number ('PIN') and password for banking and other online transactions. The way in which electronic signatures are authenticated can also vary, depending upon the type of signature.

[7.2.1.3] The question remains whether an electronic signature can serve just as well as a handwritten signature to authenticate a document, that is, it identifies the signatory, that it evidences the party's approval of the content of the document and it provides integrity for the contract between the parties ensuring the reliability and admissibility of the parties agreement.[920]

[7.2.1.4] Legislation, such as the *Electronic Transactions Act 1999* (Cth) and its state

[916] *Toll (FGCT) Pty Ltd v Alphapharm Pty Ltd* (2004) 219 CLR 165 .
[917] Mason above n 192, 5.
[918] *R v Moore Ex Parte Myers* (1884) 10 VLR 322.
[919] Section [2.14.2.1] provides a more complete list: refer Christensen, Duncan & Low, above n 193, 76.
[920] *Leeman v Stocks* (1951) Ch 941 [947]-[948].

equivalents,[921] purport to give effect to electronic signatures. This legislation provides that a signature can be affixed electronically as long as the method used was reliable and can be used to identify the person.[922] Indeed, in *Getup Ltd v Electoral Commissioner*,[923] Perram J concluded that a signature affixed to an enrol-to-vote form using a digital pen applied to a laptop's trackpad, was a reliable method pursuant to *Electronic Transactions Act 1999* (Cth), sufficient for the purposes of the *Electoral Act 1918* (Cth).

[7.2.1.5] The *Electronic Transactions Acts* were enacted as part of the government's 'strategic framework for the development of the information economy in Australia, and is based on the *United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce of 1996.* The purpose of the legislation is to give effect to transactions, notwithstanding they may be conducted via electronic communications.

[7.2.1.6] The analysis in section 2.14 highlighted that some commentators[924] doubt whether electronic signatures can yet replace the traditional handwritten signature on hard copy for transactions for the disposition of an interest in land. This is because there are still some question marks over whether the technology and the law provide enough certainty, given the propensity for fraud.

[7.2.1.7] It appears the only way in which there can be some way to ensure the integrity of an electronic signature, is to use an encrypted digital signature as part of a Public Key Infrastructure ('PKI'). Digital signatures within the realm of a PKI use digital key pairs, a private key and a public key, with the public key being held by a Certification Authority ('CA') who can vouch for the identity of the signatory. The complication is that the CA itself needs to be verified. To explain, digital signatures operate by using cryptography, which arguably increases the reliability of the digital signature. However, there are still issues with digital signatures, depending upon the method used. As explained by Mason,[925] there are two types

[921] *Electronic Transactions Act 2000* (NSW), *Electronic Transactions Act 2000* (Vic), *Electronic Transactions Act 2001* (Qld), *Electronic Transactions Act 2000* (SA), *Electronic Transactions Act 2011* (WA), *Electronic Transactions Act 2000* (Tas), *Electronic Transactions Act 2001* (ACT), *Electronic Transactions Act* (NT).
[922] *Electronic Transactions Act 1999* (Cth) s 10(1), *Electronic Transactions Act 2000* (NSW) s 9(1), *Electronic Transactions Act 2000* (Vic) s 9(1), *Electronic Transactions Act 2001* (Qld) s 14(1), *Electronic Transactions Act 2000* (SA) s 9(1), *Electronic Transactions Act 2011* (WA) s 10(1), *Electronic Transactions Act 2000* (Tas) s 7(1), *Electronic Transactions Act 2001* (ACT) s 9(1), *Electronic Transactions Act* (NT) s 9(1).
[923] [2010] FCA 869.
[924] Christensen, Duncan & Low, above n 193.
[925] Mason, above n 192, 261-266.

of cryptographic systems: symmetric and asymmetric.

[7.2.1.8] Symmetric cryptography uses the same key, or cipher, for both encryption and decryption. Ostensibly, an encrypted message is safe to send, because an interceptor would be unable to decrypt the message without the key. There can be problems with secure transportation of the key to the recipient of the message so they can decrypt it; another use disadvantage is when messages are to be sent to large number of people, that is, how do you keep the cypher secure?

[7.2.1.9] With asymmetric cryptography, there are a pair of keys, a 'public' key and a 'private key'. The public key can be distributed, while the private key must be kept secret by the key owner. With key pairs, one operation, such as encryption, can be done with the public key while the other operation, decryption, can only be done with the corresponding private key.

[7.2.1.10] The message is signed using the private key. First a hash code, which is a unique numerical value generated by an algorithm, of the content is generated so that the system will know if the content has changed during delivery. The hash code is then 'signed' with the private key. The recipient uses the public key to verify the 'signed' hash code that has been sent. If the hash codes match, the message is verified. This works as long as the private key remains secure and secret and is not compromised.

[7.2.1.11] There are still problems in using digital signatures. One problem is that the recipient needs to be sure the sender is who they say they are. One solution to this problem is to use a Public Key Infrastructure ('PKI'), where the public key can be placed with a Certification Authority ('CA') who can certify a person's identity. The question here is, who certifies the CA? Another problem is that of non-repudiation, that is, that once someone has digitally signed an electronic communication, that they cannot deny the fact that they did sign it. Mason[926] sets out other problems with PKI, such as lack of standards within the industry.[927] Further, there are inherent weaknesses with digital signatures, like the vulnerability of passwords used with the private key,[928] not to mention the inherent weaknesses with the technology, in that any system can ostensibly be hacked. Further, how does one attribute

[926] Mason, above n 192.
[927] Ibid at 285.
[928] Ibid at 286.

actions recorded in digital format to a specific human being?

[7.2.1.12] No method is failsafe, and certainly, handwritten signatures have been applied fraudulently over the years. However, it appears we are yet to have in place one standard, reliable system for use of digital signatures.

[7.2.1.13] The Electronic Conveyancing National Law ('ECNL'), as explained in section 2.14.6, allows for a lawyer to sign to effect a transfer of land on behalf of their client. There are stringent rules around the application of the ECNL, and the technology used appears robust, however, it will be some time before the parties to the transaction themselves may sign contracts electronically.

[7.2.1.14] It is submitted that for contracts that do not deal with the disposition of an interest in land, electronic signatures can be admitted and a court can weigh up the evidence in order to authenticate electronic signatures. However, with signatures for land contracts, it is submitted it is prudent to wait for further changes to the ECNL that allow for the parties to the contract to sign documents electronically, and for technology that will allow digital signatures to be applied in a way that can reasonably guarantee the identity of the signor.

[7.2.1.15] In Australia, some government departments, such as Medicare and the Australian Taxation Office, provide digital certificates based on the Gatekeeper (Public Key Infrastructure) framework. For example, health care professionals can obtain a Medicare Public Key Infrastructure (PKI) certificate to access online services. These systems only go some way towards using digital signatures in a meaningful way. The problem of many CA's is not addressed, and until the government appoints one agency to be responsible for digital signatures, in much the same way as there is one agency responsible for passports, this problem will remain.

[7.2.1.16] Until these issues are resolved, whether through better technology and/or legislative changes, paper versions of land contracts, signed by the parties to be charged, will continue in the short term.

7.3 The Definition of 'Document'

Question 2:
Is the definition of 'document' in the Uniform Evidence Acts adequate for the purposes of electronic evidence and, in particular, does it appropriately identify the nature of electronic evidence in that it comprises both content and storage media?

[7.3.1.1] At common law, a document does not necessary need to have paper as a medium of proof.[929] Prior to the advent of computers, the most common form of document was paper, although cases have recognised documents inscribed on stone, marble, clay or even metal'.[930]

[7.3.1.2] The existing definition of 'document' in the *Uniform Evidence Act*, is broad enough to include documents created and stored on all forms of electronic media. An analysis of case law in section 4.3 demonstrates that information contained on electronic media is included in the broad definition of document in the *Uniform Evidence Act*. However, with respect, the courts do not appear to distinguish the fundamental difference between paper and electronic documents. Firstly, an electronic documents requires a storage medium upon which to store the content, and secondly, a 'document' may indeed be stored across more than one storage medium. It is, indeed, the computer software that compiles the document to be used in evidence.

[7.3.1.3] As identified by the Sedona Conference, there are a number of key differences between paper and electronic documents, which include (a) metadata, (b) volume and duplicability, (c) persistence, (d) dynamic, changeable content, (e) environment dependence and obsolescence and (f) dispersion and searchability.[931] Metadata is a key point of difference, as often metadata contained in an electronic document, cannot be seen when the document is printed, and this metadata may contain crucial evidence. Courts have recognised that electronic records that are printed and retained, rather than being retained in their electronic format, are 'dismembered' documents.[932]

[7.3.1.4] Since the advent of the personal computer in 1976, a whole new paradigm in

[929] *R v Daye* [1908] 2 KB 333, 340.
[930] Ibid.
[931] The Sedona Principles Best Practices Recommendations and Principles Addressing Electronic Document Production (2nd ed: 2007), at <http://www.thesedonaconference.org> at 11 September 2015.
[932] *Armstrong v Executive Office of the President* 1 F.3d 1274 (D.C. Circuit Court of Appeals 1993).

the way in which information is created and exchanged, has evolved. The internet is a world-wide network of computers that can 'talk to' each other using communication protocols such as TCP/IP (transmission protocol/Internet protocols). Email and social media are now becoming the default method of communication, notwithstanding that evidentially, social media content is complex. While technically covered under the broad definition of 'document', evidence from social media can be difficult to authenticate because (a) it may not be possible to establish the identity of the person who created the 'document' and (b) a 'document' can be authored by more than one person and (c) the evidence may be later removed by the creator. Email has been recognised as a record keeping system.[933]

[7.3.1.5] Cloud computing, where an individual or organisation 'rents' computer space from a cloud provider, is rapidly becoming an accepted method of data storage. Cloud computing can raise questions about ownership of data, the maintenance of integrity, the protection of privacy and jurisdictional issues, since many cloud providers can have servers located outside of Australia.

[7.3.1.6] As Paul notes, 'the modern electronic file lives not as an artifact one can hold in one's hand, but as pure information that can be reordered at will'.[934] In Chapter 4, the existing case law that had considered electronic evidence, was examined. In Australia, there seems to be a general assumption that a 'CD-Rom' or a 'hard drive' is a document, simply because it is an electronic device, rather than a recognition that the storage medium and the content are separate, yet bound to one another. In England and Wales, and in the United States of America, the case law regarding electronic evidence appears inconsistent. Conversely, the courts in Canada, do appear to recognise the difference between content and storage media.

[7.3.1.7] Even if this distinction were widely recognised by the Australian courts, another issue is that electronic media contains many documents, some of which may be privileged, confidential or irrelevant, and presently, the only way to have the relevant documents separated, is to engage an independent expert. There are many types of storage media, and the way in which electronic data are stored, means that one document could be stored on more than one storage media. In order to retrieve the information that comprises a document, a complex

[933] *Australian Competition and Consumer Commission v Air New Zealand Limited* (No 1) (2012) 301 ALR 326 [57] per Perram J.
[934] Paul, above n 25, 48.

process involving many pieces of software operating across various storage media, is required to bring the data together to, in turn, generate the electronic document.

[7.3.1.8] While the case law indicates an inconsistent approach of courts, there are some notable judicial exceptions, as set out in sections 3.1, 3.3.8 and 5.4.5, which demonstrate an understanding and recognition of the fundamental differences between paper and electronic evidence.

[7.3.1.9] While the case law may be deficient, there are legislative provisions in other jurisdictions that do offer some assistance; these legislative provisions are summarised in Appendix B.

[7.3.1.10] The *Federal Rules of Evidence* (USA) do provide an extensive definition of electronic data, which appears to be all inclusive, and the *Civil Procedure Rules* (Eng) have been amended to cater for electronic documents, however, it is submitted that neither of these go far enough towards recognising that it is the system within which electronic documents are created, that is essential when examining whether electronic documents are authenticated or not.

[7.3.1.11] The definition contained in the *Civil Procedure Rules 2005* (Eng) provides that a 'document' includes anything in which information of any description is recorded,[935] It broadly defines an 'electronic document' to include email and other electronic communications such as text messages and voicemail, word-processed documents and databases and documents stored on portable devices as well as documents that are readily accessible from computer systems and other electronic devices and media, including documents stored on servers, backup-up systems and documents that have been deleted. It also includes metadata and other embedded data which is not visible on a computer screen or on a print out.

[7.3.1.12] The *Uniform Electronic Evidence Act 1998* (Can) contains definitions of 'data', 'electronic record' and 'electronic records system'. It is submitted that the definitions contained in that legislation are much more reflective of the unique nature of electronic evidence, than

[935] In England & Wales, the *Data Protection Act 1998* (Eng), Part 1(a) to (c) make it clear that information that is recorded on a computer, or is intended to be held on a computer, is data. Data is also information recorded on paper if it is intended that it is to be put onto a computer.

any of the definitions currently contained in the Australian *Uniform Evidence Acts*.

[7.3.1.13] To reiterate these provisions of the *Uniform Electronic Evidence Act 1998* (Can), they are:

- 'Data' means representations, in any form, of information or concepts.
- 'Electronic Record' means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.
- 'Electronic Records System' includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records.

[7.3.1.14] It is submitted that the definitions contained within the *Uniform Evidence Acts* should be extended to cover electronic documents and records. Definitions should be included that are similar to those contained in the *Uniform Electronic Evidence Act 1998* (Can). If definitions of 'data', 'electronic record' and 'electronic records system' are included in the *Uniform Evidence Acts*, this will go a long way to recognising that electronic documents are stored and created as part of a computer system.

[7.3.1.15] Interestingly, neither the *Evidence Act 1985* (Can), nor the *Uniform Electronic Evidence Act 1998* (Can) contain a definition of 'document'. The former Act does define 'record' as it pertains to business records, as including the whole or any part of any book, document, paper, card, tape or other thing on or in which information is written, recorded, stored or reproduced.

[7.3.1.16] However, it is submitted that the *Uniform Evidence Acts* should be amended to widen the meaning of 'document' to specifically include electronic documents, rather than simply containing the imprecise, and rather confusing, current definition.

[7.3.1.17] It is submitted that a definition similar to that contained in the *Civil Procedure Rules 2005* (Eng), should be considered for inclusion in the *Uniform Evidence Acts*. That definition provides that a 'document' includes anything in which information of any

description is recorded.[936] It includes a definition of an 'electronic document' which specifies email and other electronic communications such as text messages and voicemail, word-processed documents and databases and documents stored on portable devices as well as documents that are readily accessible from computer systems and other electronic devices and media, including documents stored on servers, backup-up systems and documents that have been deleted. It also includes metadata and other embedded data which is not visible on screen or on a print out.

7.4 Business Records Exception

Question 3: Should the Business Records Exception, in its present form in the *Uniform Evidence Acts*, continue to apply to electronic evidence, or does it need modification?

[7.4.1.1] The common law Business Records Exception is now embodied in the *Uniform Evidence Acts* s 69.

[7.4.1.2] The Business Records Exception arose on the presumption that records created by employees in the course of their employment were generally accurate, certainly far more accurate than human memory. Further, the Business Record Exception was built around the practice where an employee would update a hard copy record, such as a ledger or other hard copy book, and enter records consecutively. With electronic business records that are created and stored in computer systems, this is no longer the case. Business records are created and stored in any number of software programs, and are accessible and updated by any number of employees, in disparate locations. While it is true that such records, as long as they are kept in the ordinary course of business, and are far more reliable than a witnesses' memory, it is submitted that, in addition to the evidence itself, it should be demonstrated that there is a reasonable level of security around the computer system itself, in order to show that the evidence is authentic.

[7.4.1.3] Of course, the premise behind the Business Records Exception that records

[936] In England & Wales, the *Data Protection Act 1998* (Eng), Part 1(a) to (c) make it clear that information that is recorded on a computer, or is intended to be held on a computer, is data. Data is also information recorded on paper if it is intended that it is to be put onto a computer.

created in the ordinary course of business are likely to be more correct than relying on a witness's memory of an event that might have occurred years previously, is a sound one. Otherwise, much court time would be taken up by a party having to prove how every single document was created. However, the rules under which such evidence is admitted, need to be backed up by an understanding of how electronic evidence is created and stored, and not simply apply old rules that were developed around paper evidence.

[7.4.1.4] With electronic evidence created as part of a computer system within a business, generally, one person cannot give evidence as to the creation and content of that electronic evidence. Paul[937], in particular, uses the example of a contract in a word processing format stored on a computer network within a company comprising 1,500 employees. Although a senior manager can attest to the content of the contract which may have been drafted several years' previously, with the manager's input, the manager cannot testify to the exact wording of any specific section of the contract without reference to it, nor can the manager testify to the systems used to store, backup up, audit and generally the integrity of the document. How can the manager affirm that the document was not accessed by one of the other 1,500 employees? Unless the manager is also the IT administrator, and that all of the required security elements are in place, the manager has no knowledge as to the integrity of the document. Similarly, if an employee enters records into a database, it is submitted that that employee cannot also then verify that the database record itself has not been changed since the entry was made.

[7.4.1.5] It is the Business Records Exception that is most subject to scrutiny when examining the authentication of electronic evidence. This is because generally, the witness tendering the evidence is not the person who created the evidence. A court needs to be assured that from the time the record was created, to the time it is tendered in court, the record was kept reasonably secure, and that the evidence was not at undue risk of tampering. It is submitted that a witness attesting as to the records of a business should also be in a position to know how and where the records are stored, and be responsible for their safe custody, and if they are not, suggest another witness who is able to attest to this. Otherwise, the authenticity of the evidence may be open to challenge.

[7.4.1.6] The concept of the Business Records Exception should not change. The

[937] Paul, above n 25.

principles around the rule are to ensure evidence can be admitted if there is no challenge to it. However, it is submitted that the rule itself should be modified to reflect evidence created as part of a computer system. The way in which a witness's evidence is given needs to change in order to demonstrate that the computer system in which the records were created were reasonably secure so that, there is little risk that the records were altered between the time of creation and the admission the of evidence in court.

[7.4.1.7] The *Uniform Electronic Evidence Act 1998* (Can) s 5, which is stated in section [7.7.1.10] above is re-stated below:

> 5. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed [in any legal proceeding]:
>
> a. by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;
>
> (b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or
>
> (c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

[7.4.1.8] Section 5(c) is particularly relevant in this day and age, where many electronic records are stored with third party providers, such as Cloud providers. This means a party cannot simply say they are not their records simply because the storage of the records has been outsourced.

7.5 Integrity of Documents During Discovery

Question 4: Does the discovery process provide sufficient safeguards to ensure that the integrity of evidence remains intact?

[7.5.1.1] Discovery can be a crucial step in litigation. It is imperative that, during discovery, documentary evidence is collected in a way which does not destroy its integrity, the chain of custody from the time of collection to the presentation of evidence in court can be lost, which can affect a document's authenticity. With electronic evidence, users can unwittingly change metadata, with the consequence that the integrity of the evidence is compromised.

[7.5.1.2] Each jurisdiction has its own rules and practice directions that govern discovery, and these are set out in Chapter 5. The various rules of court dictate how and when documents should be discovered during the litigation process, and this is not something that is dealt with pursuant to the *Uniform Evidence Acts*. The *Uniform Evidence Acts* are concerned with ensuring that only relevant and authenticated documents are admitted as evidence. If, during the discovery process, electronic documents have not been collected in a way that ensures their evidential integrity, this will have an impact on their admissibility. Most of the rules and court practice notes concern hard copy documents and those that do consider electronic documents, do not, it is submitted, go far enough in recognising the unique characteristics of electronic evidence, compared to hard copy.

[7.5.1.3] Discovery of documents that are in the possession or control of a party, can be ordered by the other party or parties to the proceedings. The question of control is an important one when considering electronic evidence. In the English Court of Appeal, a database was held to be intangible,[938] and therefore, incapable of being property which could be 'possessed'. In the New Zealand Court of Appeal[939] the court considered that a digital video file could not be 'property' pursuant to the definition in the *Crimes Act 1961* (NZ), while arguably, a hard drive could be property. The court concluded that 'electronic footage stored on a computer is indistinguishable in principle from pure information'.[940] However, this is incongruous with the laws of intellectual property where intangible rights can be infringed. The law is clearly in a state of flux, with no clear answer.

[7.5.1.4] With respect to metadata, a recent case before the Commonwealth Privacy Commissioner,[941] brought by a Sydney Morning Herald journalist proved the point that anyone can access their own metadata that is now being kept by telecommunications service providers. However, this issue of ownership of, and access to, metadata has not yet been considered by a higher court in Australia.

[7.5.1.5] The analysis in Chapter 5 demonstrates that there is a need for a review of the law about possession and control of electronic evidence.

---

[938] *Your Response Limited v Datateam Business Media Limited* [2014] EWCA Civ 281.
[939] *Dixon v R* [2014] NZCA 329 (7 July 2014).
[940] Ibid [551].
[941] *Benn Grubb and Telstra Corporation Limited* [2015] AICmr [35] (1 May2015).

[7.5.1.6] Cases involving social media, and gaining access to such evidence, are also discussed in Chapter 5, with each case being decided on a case by case basis. Social media, as evidence, is complex in ways that cannot be compared with hard copy evidence, given the dynamic nature of social media and issue with proving identity.

[7.5.1.7] Another point highlighted by the analysis in Chapter 5 is that of Technology Assisted Review being used during discovery. The tools that are now available to assist lawyers are well designed and reliable, however, there continues to be a lack of understanding amongst lawyers and the judiciary of how these tools work, and why they assist to reduce overall costs of discovery and to aid lawyers in finding the relevant evidence for their clients.

[7.5.1.8] It is submitted that the practice notes referred to in Chapter 5 do not go far enough in analysing the nature of electronic evidence, how that evidence must be treated during collection and processing, in order to preserve its integrity. Indeed, many lawyers would not, it is submitted, acknowledge the unique nature of electronic evidence and would rely on methods traditionally used to discover hard copy documents. Therefore, it is incumbent upon courts to insist upon appropriate standards and guidelines for the collection, review, analysis and presentation of electronic evidence. An international standard for the collection, processing, review, analysis and presentation of electronic evidence has been established, known as the Electronic Discovery Reference Model (EDRM), which is explained in section 5.3.3.

[7.5.1.9] Cases such as the *Da Silva Moore v Publicis Groupe*,[942], which is explained in section 5.4.5, confirm that, at least in the United States of America, lawyers should be aware of, and know how to use, appropriate legal technology to find relevant documents during discovery, so that costs are not unnecessarily incurred by reviewing electronic evidence as if it were hard copy. Such technology includes 'basic' tools such as 'de-duplication' where all identical electronic documents are removed from a review set, 'email threading', which groups emails in a 'thread' (that is where each email sent, replied to, replied to again and so on, are together), 'near duplicate detection', which identified documents that are similar but not identical. Such 'basic' tools are commonly used in electronic discovery. However, the more 'complex' tools such as clustering, concept searching and predictive coding, which are

[942] 11-civ-1279 (ALC) (AJP), U.S. Dist. LEXIS 23350 (S.D.N.Y. Feb. 24, 2012).

explained in section 5.4, are still gaining acceptance. It is the use of these more 'complex' tools that some members of the judiciary are encouraging, since they aid in the search for relevant documents to be used as evidence, in a much more cost effective way, compared to traditional methods. In addition to such cases, there are numerous academic studies[943] that show that the advantages of using technology to find relevant documents during discovery, compared to traditional methods of linear review, are substantial.

[7.5.1.10] Discovery involves many steps, from collection of evidence to presentation in court, and while courts in Australia have not encouraged the development of standards in the use of technology during discovery, there are examples to be drawn from the United States of America and the United Kingdom.

[7.5.1.11] The current court practice notes are silent as to the use of technology during the discovery process. Therefore, it is left to the parties to decide what to use. It is submitted that, as a starting point, the international standard known as the Electronic Discovery Reference Model (EDRM) should be formally recognised in court practice notes in Australia.

[7.5.1.12] There is no case law in Australia, similar to *Da Silva Moore v Publicis Groupe,*[944], which effectively states that lawyers are not doing their job effectively if they are not aware of, nor use, appropriate technology during discovery. The current *Uniform Evidence Acts* do not prescribe methods for discovery, rather this is left to court rules and practice directions. However, for the *Uniform Evidence Act* to work effectively in the determination of admissibility of evidence, the court rules and practice notes need to confirm that the appropriate tools be used to find relevant electronic evidence and there should be some national consistency in approach.

[943] See for example: Gordon V. Cormack and Maura R. Grossman, *Evaluation of Machine-Learning Protocols for Technology-Assisted Review in Electronic Discovery*, at: <http://www.wlrk.com/webdocs/wlrknew/AttorneyPubs/WLRK.23339.14.pdf> at 11 September 2015.
[944] 11-civ-1279 (ALC) (AJP), U.S. Dist. LEXIS 23350 (S.D.N.Y. Feb. 24, 2012).

7.6 Protection of Privilege

Question 5: For documents to which legal professional privilege applies, are there sufficient protection measures in place for retrieval of evidence on electronic media that contains privileged information?

[7.6.1.1] Legal professional privilege is described in section 5.5, and is embodied in the *Uniform Evidence Acts*. Any documents over which privilege is claimed, do not need to be disclosed to the other party during a proceeding.[945]

[7.6.1.2] At common law, the doctrine of legal professional privilege protects any statement, whether made orally or in writing, which has been created for the sole purpose of providing legal advice, or for the purpose of use in existing or anticipated litigation.[946] *Uniform Evidence Acts*¸ s 118 replaces the common law 'sole purpose test' with a 'dominant purpose test', that is, if the dominant purpose of the advice is for existing or anticipated judicial or quasi-judicial proceedings.

[7.6.1.3] Privilege can be lost if one party has been seen to have waived privilege. However, the Australian High Court recently made it clear that a lawyer has an ethical responsibility to notify the opposing side if it is apparent that documents have been disclosed inadvertently.[947] In the United States of America, some parties may enter into 'clawback agreements' whereby, if documents are inadvertently disclosed during discovery, that party does not waive any privilege that may attach. This is useful in cases where there are large volumes of electronic documents to discovery, and it is not cost effective to review every document.

[7.6.1.4] While documents that are subject to legal professional privilege do not have to be produced to the other party in a proceeding, the real issue with privilege and electronic documents is apparent when electronic media is seized, either via a search order made by a court, or via an Anton Piller order. This is because often the privileged material is mixed up with the other, relevant, material, and orders are required to protect that privileged material

[945] *Uniform Evidence Acts*, part 3.10.
[946] *Grant v Downs* (1976) 135 CLR 674.
[947] *Expense Reduction Analysts Group Pty Ltd v Armstrong Strategic Management and Marketing Pty Limited* (2013) 250 CLR 303.

before the records are made available to the requesting party. In recent years, the number of bodies with coercive information-gathering powers has increased, yet the way in which privileged and other sensitive material, has not been adequately dealt with by the legislature.

[7.6.1.5] While the Australian Law Reform Commission ('ALRC') has considered the issue and made recommendations to the effect that Federal client privilege legislation should provide that 'in the absence of any clear, express statutory statement to the contrary, client legal privilege applies to the coercive information-gathering powers of Federal bodies, and any such legislation should take into account several factors when determining whether client legal privilege may be abrogated.[948] These factors include whether the inquiry concerns a matter/s of public importance, whether the information can be obtained in a timely manner using alternative means and also the degree to which a lack of access to the privileged information will hamper or frustrate the operation of the investigation and whether the legal advice is central to the issues being considered by the investigation. While the ALRC's recommendations make practical sense, the problem seems to be that often information is seized and it is up to the party whose information has been seized, to make an application to court to protect the privileged information.

[7.6.1.6] There is a need for legal rules to treat electronic records in a different light from paper records, in that electronic records more often than not, reside in a system. How records are stored and retrieved and viewed as evidence, should be considered in light of the system itself, not a 'document' in isolation.

[7.6.1.7] It is submitted that too often, users who are not trained in evidential procedures, are required to collect and analyse data that contains potentially privileged material. To protect the integrity of the data and any privileged material, there needs to be clear rules outlining that:

(a) The system needs to be such that information is stored properly and appropriately so retrieval is done in a correct manner; and
(b) Any court order allowing access to the electronic material should clearly set out how information stored in a 'system', that does not fall within the ambit of the court order, to is be handled.

[7.6.1.8] It is submitted that guidelines need to be developed by the legislature that make

[948] Australian Law Reform Commission, *Privilege in Perspective: Client Legal Privilege in Federal Investigations*, Report 107 (2007).

it clear, how, and by whom, evidence obtained pursuant to a court order, is dealt with, in order to preserve any privilege that might apply to documents. The party receiving and reviewing such material needs to be independent of the parties to the proceedings and have sufficient knowledge and expertise to be able to handle not only privileged material, but also sensitive and confidential information.

7.7 The presumptions in *Uniform Evidence Acts* ss 146 & 147

Question 6: Do the presumptions in *Uniform Evidence Acts* ss 146 and 147 need modification to reflect the way in which electronic evidence is generated?

[7.7.1.1] The *Uniform Evidence Acts* ss 146 and 147 create rebuttable presumptions that, where a party tenders a document or thing that has been produced by a process or device, if the device or process is one that, if properly used, ordinarily produces a particular outcome, in producing the document or thing on this occasion, the device or process has produced that outcome. For example, where a scanner has made an image copy of the document, it would not be necessary to call evidence to prove that the scanner was working properly when it was used to create an image of the document. The *Uniform Evidence Acts* s 147 applies to evidence created by a device or process is or was at that time used for the purposes of the business in the course of business.

[7.7.1.2] The *Uniform Evidence Acts* ss 146 and 147 have the consequence that evidence is relatively easy to admit and its authenticity is only questioned where the other party brings it into question. Further, the presumption is that the machine or device upon which the evidence has been produced, is working correctly, and is based on the assumption that machines and devices are generally reliable. However, the question raised by this thesis, is whether that presumption, should be further extended to computer systems, not just devices and machines.

[7.7.1.3] The rationale behind the rebuttable presumptions in *Uniform Evidence Acts* ss 147 and 147 are sound, otherwise courts would be unnecessarily laden with the need to have voluminous amounts of evidence tendered in order to get documentary evidence admitted. However, are the rebuttable presumptions too wide? Should there a more strict test apply when considering evidence being tendered from computer systems, and if so, what should that test

encompass?

[7.7.1.4] Commentators such as Paul,[949] suggest that the foundational requirement for authentication of electronic evidence has largely deteriorated into a 'trivial showing', and his argument largely centres on the reliability of information that is created and stored within a computer system. Paul argues that due to the unique nature of electronic evidence, if one cannot show that the information was created and stored within a reliable system, the chain of custody necessary to show that a document is authentic is lost.[950]

[7.7.1.5] Similarly in Canada, Chasse[951] argues that counsel and courts are simply ignoring the issues posed by electronic evidence, resulting in the consequence that electronic evidence is admitted without any form of effective authentication.[952]

[7.7.1.6] In New Zealand, Judge David Harvey notes, an electronic file does not exist in itself, in that it does not exist independently from the process in which it was created.[953]

[7.7.1.7] This research has demonstrated that the rules surrounding authentication of evidence were formed around the need to authenticate paper documents. Further, the current rebuttable presumption in *Uniform Evidence Acts* ss 146 and 147 were designed to apply to evidence created by machines and devices, not necessarily computer systems. It is respectfully submitted that when the ALRC conducted its review of the *Uniform Evidence Acts* in 2005, although 'reliability' of computers was examined, there was a failure to examine and understand the true nature of electronic evidence, and need to authenticate it.

[7.7.1.8] The existing rules, including the rebuttable presumptions in *Uniform Evidence Acts* ss 146 and 147, do not, it is submitted, recognise that electronic evidence created and stored as part of a computer system is no longer two dimensional. Rather, electronic evidence is comprised of a series of electromagnetic pulses which must be stored on an electronic medium and which must be interpreted using specific software.

[7.7.1.9] Having said this, however, the intent behind the rebuttable presumptions is that

[949] Paul, above n 25.
[950] Ibid.
[951] Chasse, above n 512.
[952] Ibid.
[953] Judge David Harvey, *Collisions in the Digital Paradigm: Legal Rules and New Technologies*, 3rd Annual New Zealand Law & Technology Conference, 18 March 2015.

as long as there are no objections, electronic evidence can be admitted and then it is up to the court's discretion as to what weight is to be attached to the evidence. It is submitted that the intent behind these rebuttable presumptions is a sound one, otherwise evidentiary procedures would take up unnecessary court time. However, it is submitted that the wording of *Uniform Evidence Acts* ss 146 and 147 should be updated to reflect the fact that it is computer systems that create the evidence, not just machines and devices.

[7.7.1.10] The *Uniform Electronic Evidence Act 1998* (Can) s 5 contains the following provision:

> 5. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed [in any legal proceeding]:
>
> b. by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;
>
> (b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or
>
> (c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

[7.7.1.11] It is submitted that the above provision in *Uniform Electronic Evidence Act 1998* (Can) s 5 adequately recognises electronic evidence is created and stored as part of an computer system, and although it maintains the rebuttable presumptions, that is, 'in the absence of evidence to the contrary', it is a more accurate representation of the way in which electronic evidence is created and stored and more adequately reflects the rules of evidence for electronic documents.

7.8 Rules for Authentication

Question 7: Are the current rules of authentication for documentary evidence, adequate to apply to electronic evidence?

[7.8.1.1] If evidence is accepted into court, and it is not authentic, that affects the court's search for the truth upon which proper adjudication of issues depends, and justice cannot be properly served. Electronic evidence is subject to alteration without detection much more easily than paper, and it is this risk that must be addressed by a witness through whom any

electronic document is tendered.

[7.8.1.2] When the ALRC conducted their review in 2005, the approach that the ALRC took when considering the question whether a more rigorous test was required for the reception of evidence in electronic form, was to consider whether computer systems were reliable. After an analysis of the laws around documentary evidence and authentication, it is clear that it is not only the reliability of computers that is in issue with computer-generated evidence, but also that the integrity of the system in which documents are created and stored that should be questioned.

[7.8.1.3] Moving records from one medium to another can change the metadata within an electronic record, which in effect, changes the evidence. The inherent unreliability of software can also give rise to concern about the integrity of computer-generated evidence.

[7.8.1.4] In Australia, the cases that examine authentication of documentary evidence have generated a lengthy debate on whether a document can authenticate itself, or whether other factors must be taken into account. Comments made by Bryson J in *NAB v Rusu* were the subject of criticism by Stephen Odgers SC and in subsequent cases. However, ultimately, Austin J in *ASIC v Rich* concluded that authentication cannot be achieved solely by drawing meaning from the document where there is no other evidence to indicate provenance. In *ASIC v Rich*, documents that were printed out from a file server and which seem to be reports generated from an accounting software system, were authenticated and admitted into evidence. Austin J then considered what weight to give to these documents. However, with respect, these cases tend to miss the point.

[7.8.1.5] While the courts need to seek the truth, a fundamental point in *ASIC v Rich* was that the evidence appeared to have been generated within a computer software package. No evidence was given about how that software package worked and its track record for reliability, who had access to it, who entered data and who ostensibly could have entered data without authorisation. No evidence was given as to where the system was stored and the security around the system. As to the reports that were generated and found on the I:\ drive, no evidence was given around how these reports were generated; they just seem to have been produced from the I:\ Drive, without any evidence of their provenance. To simply say their provenance is the file server itself, fundamentally shows a complete lack of understanding of how such systems work. This highlights the need for evidence to be produced showing the whole context

in which electronic evidence is generated, stored, retrieved and produced.

[7.8.1.6] In England and Wales and in the United States of America, the case law also tends to look at authentication of evidence on a case by case basis, and the legislative provisions go some way towards providing guidance. However, it is submitted that Canada is the first jurisdiction to properly acknowledge the difference with electronic evidence, compared with paper evidence, and offer some sort of guidance on how to properly authenticate such evidence by examining the reliability of the system in which the evidence was created.

[7.8.1.7] Whether electronic evidence is authentic is left to the trier of fact to determine. In civil cases, this will usually be the judge.

[7.8.1.8] In Canada, *Uniform Electronic Evidence Act* (Can), s 3 provides that 'the person seeking to introduce an electronic record [in any legal proceeding] has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.' Canada is also a common law jurisdiction, so the rules of evidence that have developed in Canada originated in England, in the same way as Australia's rules of evidence developed. The *Uniform Electronic Evidence Act* (Can) does permit parties to adduce evidence as to 'the integrity of the electronic documents system by or in which the electronic document was recorded or stored'. There are several presumptions to show proof of integrity including (a) proof that the storage medium was operating properly; (b) proof that the document was recorded or stored or recorded and stored by an adverse party; and (c) proof that the document was recorded or stored in the ordinary course of business by a party outside the litigation. The provisions also allow for evidence to be provided of current standards, procedures and practices with regard to the integrity of the recording or storing system. Such evidence can go to the integrity of the electronic document system, but also to 'determining under any rule of law whether an electronic document is admissible' and could be used as a source of evidence of the 'reliability' of a document for hearsay purposes. Industry standards may be used to show evidence maintains integrity, although such standards are not binding on the court, they will be persuasive.

[7.8.1.9] However, whether a document is authentic can only be determined by a number of factors, principally whether the document's integrity has been compromised between the time it was created by the user and when the document is tendered as evidence. Immutability of a document is important to show authenticity, and with documentary evidence, a witness

must attest to this. For a document to be admitted pursuant to the Business Records Exception, the only way to determine authenticity is to show that the organisation took reasonable steps to preserve the integrity of the computer system upon which the document was stored and created.

[7.8.1.10] The way in which the integrity of the computer system can be demonstrated is to have appropriately qualified persons within the business provide evidence as to the standards, procedures and practices used by the organisation to record and store electronic evidence. Some of this evidence may have been created many years ago and the data in question may have been archived or migrated to new systems when the software or storage medium becomes superseded. It is the content itself that must be authentic and arguably with electronic evidence there can be no guarantee that the content has not been changed. Therefore, when authenticating records pursuant to the Business Records Exception, it must be demonstrated that the organisation made reasonable efforts to keep their computer systems secure to preserve the integrity of the content of those business records. The days of a bound hard copy volume being removed from a shelf by an employee to enter a record as part of their job have passed. Instead, many different employees may have access to documents and their contents and may be able to change the content maliciously if they have an ulterior motive to do so. Indeed, the changes made by such an employee may not be discernible without computer forensic evidence and, in any event, a party to litigation may not even realise that the contents have been changed in order to query their veracity.

[7.8.1.11] The threshold for admissibility has traditionally remained low, allowing the trier of fact to determine whether evidence should be admissible and then allowing any defects in the quality of the material to go to weight.

[7.8.1.12] While some commentators such as Chasse[954] suggest that it must be demonstrated that the computer system itself is secure, however, it is submitted that what is required is a level of reasonableness, and the current wording of the *Uniform Evidence Act* does not go far enough to achieve this outcome. It is highly probable that documents can be, and are, admitted into evidence that do not meet the requirements of authentication. Today, electronic documents that are sought to be admitted pursuant to the Business Records Exception to the Hearsay Rule, are not subject to even a basic requirement to show that the

[954] Chasse, above n 512.

computer system on which those records were created has even a reasonable level of security to protect their integrity. This requirement does not have to be onerous, but it should require that the person through whom the evidence is being tendered, to be capable of demonstrating the security around the computer systems upon which the business records were created and stored. If the documents have been archived and created in a superseded software program, this may also be relevant.

[7.8.1.13] With respect to integrity of the document, *Uniform Electronic Evidence Act* (Can), s 4(1) provides that '[In any legal proceeding,] Subject to Subsection (2), where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.' This section was worded this way because with electronic records, it is difficult to identify the original document. The emphasis is on the system in which the records is kept, not the record itself. There is a presumption of integrity in the *Uniform Electronic Evidence Act* (Can) s 5 which provides that 'in the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed [in any legal proceeding]'. This means that there is a presumption that the computer system upon which the record is stored is operating properly, although the security around the system may be subject to attack. This section enables records to be admitted where there is no argument as to their reliability. For example, a small business that uses standard off-the-shelf software for its record keeping, would meet this threshold. However, if the small business did not have standard security around its record keeping system, such as a password protected files, this may open up the records to an attack on integrity.

[7.8.1.14] The *Uniform Electronic Evidence Act* (Can), section 5 provides further sub-sections:

> (a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;
> (b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or
> (c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

[7.8.1.15] The *Uniform Electronic Evidence Act* (Can) s 6 provides that 'for the purpose

of determining under any rule of law whether an electronic record is admissible, evidence may be presented [in any legal proceeding] in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or stored, having regard to the type of business or endeavour that used, recorded or stored the electronic record and the nature and purpose of the electronic record.'

> The current system of foundations allows litigants to place into evidence almost anything they want so long as they can get a witness with some nexus to testify that a document is what it is claimed to be. They can employ a sort of legerdemain. If we are to be intellectually honest, there is almost no preliminary burden of providing digital information is authentic. [955]

[7.8.1.16] The matters referred to in subsection 4(2) and sections 5 and 6 may be established by an affidavit given to the best of the deponent's knowledge or belief.

[7.8.1.17] It is submitted that the current rules of evidence do not adequately safeguard the proper authentication of electronic evidence. While the courts must retain the discretion to admit evidence, and then consider what weight it might have, the fact remains they are still considering electronic evidence in the same way as they consider hard copy evidence. There should be a recognition in the rules of evidence that electronic evidence is created as part of a computer system and that the integrity of the computer system from which the electronic evidence was produced is essential to proving the integrity of the evidence itself. It is the integrity of the computer system to witness should attest when authenticating a document or documents.

[7.8.1.18] The *Uniform Electronic Evidence Act* (Can) s 6, as set out above in section [7.8.1.15], requires evidence that the computer system was operating properly such that the integrity of the evidence remains intact. In civil proceedings, this would need to be shown on the balance of probabilities. It is submitted that an amendment to the *Uniform Evidence Acts* that requires the witness to attest to the computer system in which the document was stored, is required. However, it is further submitted that any amendment to the *Uniform Evidence Acts*, should include an additional requirement would be that the witness attest to the fact that the computer system contained a reasonable level of security to prevent attacks from viruses and malware and other unauthorised access. Again, this would need to be proved on the balance

[955] Paul, above n 25, 49.

of probabilities.

[7.8.1.19] In a modern well run business, it could be said that a reasonable manager would employ standard computer software to protect against viruses and malware, that adequate firewall protection is in place, and that only authorised users were given access to the system. Of course, one can never completely prevent a malicious users such as a 'hacker' from breaching security, however, the security employed would need to be reasonable for the systems of the day.

7.9 Opportunities for further work

[7.9.1.1] This thesis summarises the legal position to date on the authentication of electronic evidence. It is submitted that while the *Uniform Evidence Acts*, in their currently form, may be adequate to admit electronic evidence, some changes are required in order to properly recognise that electronic evidence is fundamentally different to paper, and that when evidence is given by witnesses as to the integrity of the computer system in which the evidence was created, the witness should provide evidence as to how integrity can be reasonably relied upon.

[7.9.1.2] To summaries the opportunities for further work, these are as follows:

A Further work on an effective digital signature regime so a digital signature can replace traditional handwritten signature on paper, which is capable of non-repudiation, and that meets the *Statute of Frauds* requirements.

B Updates to the *Uniform Evidence Acts* so that:

(1) The definitions reflect the true nature of electronic evidence.

(2) A witness must attest to the reasonable level of security around the computer system in which electronic evidence was created.

(3) The rebuttable presumptions reflect the true nature of electronic evidence.

C Updates to the current discovery process to reflect international standards, and the use of technology to reduce costs of discovery.

D Further work on protection of documents to which legal professional privilege applies where electronic evidence media is seized.

E Further work to ensure there is a recognition by the legal profession in Australia that electronic evidence is different to paper and in order to properly authenticate electronic evidence, different questions need to be asked, when calling into question the authenticity of electronic evidence, compared with paper evidence.

APPENDIX A

Table 1: Definition of 'document' in Australian Evidence Acts

State or Territory	Definition
Commonwealth[956], New South Wales[957], Victoria[958], Tasmania[959] the Australian Capital Territory[960] and the Northern Territory[961] *Uniform Evidence Acts*	any record of information, and includes: (a) anything on which there is writing; or (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or (d) a map, plan, drawing or photograph.
Queensland *Evidence Act 1977 (Qld)* [962]	'document' includes, in addition to a document in writing-- (a) any part of a document in writing or of any other document as defined herein; and (b) any book, map, plan, graph or drawing; and (c) any photograph; and (d) any label, marking or other writing which identifies or describes anything of which it forms part, or to which it is attached by any means whatever; and (e) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and (f) any film, negative, tape or other device in which 1 or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and (g) any other record of information whatever. This corresponds with the definition of 'document' under the *Acts Interpretation Act 1954* (Qld):[963] (a) any paper or other material on which there is writing; and (b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for a person qualified to interpret them; and (c) any disc, tape or other article or any material from which sounds, images, writings or messages are capable of being produced or reproduced (with or without the aid of another article or device).
South Australia *Acts Interpretation Act 1915* (SA)[964]	'document' includes— (a) any paper or other material on which there is writing; and

[956] *Evidence Act 1995* (Cth) s 3 (definition of 'document').
[957] *Evidence Act 1995* (NSW) s 3 (definition of 'document').
[958] *Evidence Act 2008* (Vic) s 3 (definition of 'document').
[959] *Evidence Act 2001* (Tas) s 3 (definition of 'document').
[960] *Evidence Act 2011* (ACT) s 3 (definition of 'document').
[961] *Evidence (National Uniform Legislation) Act* (NT) s 3 (definition of 'document').
[962] *Evidence Act 1977* (Qld) s 3 (definition of 'document').
[963] *Acts Interpretation Act 1954* (Qld) s 36 (definition of 'document').
[964] *Acts Interpretation Act 1915* (SA) s 4 (definition of 'document'), for *Evidence Act 1929* (SA).

State or Territory	Definition
	(b) any map, plan, drawing, graph or photograph; and (c) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and (d) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device;
Western Australia *Interpretation Act 1984 (WA)* [965]	'document' includes any publication and any matter written, expressed, or described upon any substance by means of letters, figures, or marks, or by more than one of those means, which is intended to be used or may be used for the purpose of recording that matter.

[965] *Interpretation Act 1984* (WA) s 5 (definition of 'document'); for *Evidence Act 1906* (WA).

APPENDIX B

Table 2: Definition of 'document' in other jurisdictions

State or Territory	Definition
England & Wales *Civil Procedure Rules* 2005 (Eng) [966]	In this part – 'document' means anything in which information of any description is recorded. Moreover, 'copy', in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly. This definition is further qualified in Practice Direction 31B where a definition of 'electronic document', is also provided. This definition states that an 'electronic document' is:[967] any document held in electronic form. It includes, for example, e-mail and other electronic communications such as text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones. In addition to documents that are readily accessible from computer systems and other electronic devices and media, it includes documents that are stored on servers and backup systems and documents that have been deleted. It also includes Metadata and other embedded data which is not typically visible on screen or a print out.
**United States of America	There are 50 states within the United States of America, each with their own jurisdiction and rules of evidence. It is not intended that the rules of evidence within each state be examined, rather only the rules of evidence within the Federal jurisdiction. The rules of evidence within the United States of America are governed by the *Federal Rules of Evidence* (USA), which are quite broad and which do not appear to have a specific definition of 'document'. Therefore, it is useful to examine the *Federal Rules of Civil Procedure* (USA) which refer to the discovery of documents and more importantly, electronically stored information (ESI). The Duty to Disclose; General Provisions Governing Discovery under the *Federal Rules of Civil Procedure* (USA)[968] regulate the production of evidence in litigation in the United States of America. Rules 26 and 34 are the critical rules governing the discovery of electronic information. These rules make electronic information available for broad discovery but provide some significant safeguards for the producing party. Rule 26 is the provision governing discovery and the duty of disclosure. It mandates that all parties in litigation must disclose:[969] (ii) a copy—or a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody,

[966] *Civil Procedure Rules* 2005 (Eng) r. 31.4.
[967] Ibid.
[968] *Federal Rules of Civil Procedure* (USA) Fed. R. Civ. P, § 26, 34 (Cornell University Law School, 2010).
[969] *Federal Rules of Civil Procedure* (USA) Fed. R. Civ. P, § 26(a)(1)(B) (Cornell University Law School, 2010).

State or Territory	Definition
	or control and may use to support its claims or defenses, unless the use would be solely for impeachment Rule 34 mandates the production of documents and states that a party may serve on any other party a request within the scope of discovery provided in rule 26. This request may be to produce and permit the requesting party or its representative to inspect, copy, test or sample:[970] any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or any designated tangible things in the responding party's possession, custody or control. These rules manifest that the United States of America has recognised the prevalence of electronic evidence in litigation, however, the case law (discussed later) reveals that the courts have not adopted a consistent approach in applying the rules.
Canada *Canada Evidence Act.*[971]	'electronic document' is defined as: data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print out or other output of that data. The Act also provides that an '*electronic documents system':*[972] includes a computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic documents. The *Supreme Court Rules* in British Columbia defines document as having 'an extended meaning and includes a photograph, film, recording of sound, any record of a permanent or serious permanent character and any information recorded or stored by means of any device'.[973] The civil procedure rules in each province also have their own definitions. The *Canada Evidence Act* also provides for application of the best evidence rule in relation to electronic documents. Section 31.2(1) provides that the best evidence rule in respect of an electronic document

[970] Ibid s 34(a)(1)(A) (Cornell University Law School, 2010).
[971] *Canada Evidence Act*, (R.S.C., 1985, c. C-5) s 31.8
[972] Ibid s 31.8.
[973] *Court Rules Act*, SBC 2009 c C-5, s1.

State or Territory	Definition
	is satisfied:[974] (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or (b) if an evidentiary presumption established under section 31.4 applies (these apply to the presumption of electronic signatures). Section 31.3 provides that in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven: (a) by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system; (b) if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or (c) if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it.[975] Whilst a number of statutes in different jurisdictions have provided broad and varied definitions of 'document', several cases purport to interpret the definition of a 'document'.

[974] *Canada Evidence Act* (R.S.C., 1985, c. C-5) s 31.2(1).
[975] Ibid s 31.3.

APPENDIX C

Table 3: Business Records Exception to the Hearsay Rule in Australia

State or Territory	Definition
Commonwealth, New South Wales, Victoria, Tasmania *Uniform Evidence Acts*	Section 69 Uniform Evidence Acts provide: (1) This section applies to a document that: (a) either: (i) is or forms part of the records belonging to or kept by a person, body or organisation in the course of, or for the purposes of, a business; or (ii) at any time was or formed part of such a record; and (b) contains a previous representation made or recorded in the document in the course of, or for the purposes of, the business. (2) The hearsay rule does not apply to the document (so far as it contains the representation) if the representation was made: (a) by a person who had or might reasonably be supposed to have had personal knowledge of the asserted fact; or (b) on the basis of information directly or indirectly supplied by a person who had or might reasonably be supposed to have had personal knowledge of the asserted fact. (3) Subsection (2) does not apply if the representation: (a) was prepared or obtained for the purpose of conducting, or for or in contemplation of or in connection with, an Australian or overseas proceeding; or (b) was made in connection with an investigation relating or leading to a criminal proceeding. (4) If: (a) the occurrence of an event of a particular kind is in question; and (b) in the course of a business, a system has been followed of making and keeping a record of the occurrence of all events of that kind; the hearsay rule does not apply to evidence that tends to prove that there is no record kept, in accordance with that system, of the occurrence of the event. (5) For the purposes of this section, a person is taken to have had personal knowledge of a fact if the person's knowledge of the fact was or might reasonably be supposed to have been based on what the person saw, heard or otherwise perceived (other than a previous representation made by a person about the fact).
Queensland *Evidence Act 1977 (Qld)*	Section 92 Admissibility of documentary evidence as to facts in issue (1) In any proceeding (not being a criminal proceeding) where direct oral evidence of a fact would be admissible, any statement contained in a document and tending to establish that fact shall, subject to this part, be admissible as evidence of that fact if— (a) the maker of the statement had personal knowledge of the matters dealt with by the statement, and is called as a witness in the proceeding; or (b) the document is or forms part of a record relating to any undertaking and made in the course of that undertaking from information supplied (whether directly or indirectly) by persons who had, or may reasonably

State or Territory	Definition
	be supposed to have had, personal knowledge of the matters dealt with in the information they supplied, and the person who supplied the information recorded in the statement in question is called as a witness in the proceeding. (2) The condition in subsection (1) that the maker of the statement or the person who supplied the information, as the case may be, be called as a witness need not be satisfied where— (a) the maker or supplier is dead, or unfit by reason of bodily or mental condition to attend as a witness; or (b) the maker or supplier is out of the State and it is not reasonably practicable to secure the attendance of the maker or supplier; or (c) the maker or supplier can not with reasonable diligence be found or identified; or (d) it can not reasonably be supposed (having regard to the time which has elapsed since the maker or supplier made the statement, or supplied the information, and to all the circumstances) that the maker or supplier would have any recollection of the matters dealt with by the statement the maker made or in the information the supplier supplied; or (e) no party to the proceeding who would have the right to cross-examine the maker or supplier requires the maker or supplier being called as a witness; or (f) at any stage of the proceeding it appears to the court that, having regard to all the circumstances of the case, undue delay or expense would be caused by calling the maker or supplier as a witness. (3) The court may act on hearsay evidence for the purpose of deciding any of the matters mentioned in subsection (2)(a), (b), (c), (d) or (f). (4) For the purposes of this part, a statement contained in a document is made by a person if— (a) it was written, made, dictated or otherwise produced by the person; or (b) it was recorded with the person's knowledge; or (c) it was recorded in the course of and ancillary to a proceeding; or (d) it was recognised by the person as the person's statement by signing, initialling or otherwise in writing.
Western Australia *Interpretation Act 1984* (WA)	79C . Documentary evidence, admissibility of (1) Subject to subsection (2), in any proceedings where direct oral evidence of a fact or opinion would be admissible, any statement in a document and tending to establish the fact or opinion shall, on production of the document, be admissible as evidence of that fact or opinion if the statement — (a) was made by a qualified person; or (b) directly or indirectly reproduces or is derived from one or other or both of the following — (i) information in one or more statements, each made by a qualified person; (ii) information from one or more devices designed for, and used for the purpose of, recording, measuring, counting or identifying information, not being information based on a statement made by any person.

State or Territory	Definition
	(2a) Notwithstanding subsections (1) and (2), in any proceedings where direct oral evidence of a fact or opinion would be admissible, any statement in a document and tending to establish the fact or opinion shall, on production of the document, be admissible as evidence of that fact or opinion if — (a) the statement is, or directly or indirectly reproduces, or is derived from, a business record; and (b) the court is satisfied that the business record is a genuine business record.
Northern Territory *Evidence (National Uniform Legislation) Act 2011* (NT)	
Australian Capital Territory *Evidence Act 2011* (ACT)	

Bibliography

Texts

A Ligertwood, *Australian Evidence* (LexisNexis Butterworths, 4th ed, 2004).....167

Andreas Heusler, *Institutionen des deutschen Privatrechts* (Duncker & Humblot, Germany, 1885) 17

David J Harvey, *The Law Emprynted and Englysshed, The Printing Press as an Agent of Change in Law and Legal Culture 1475-1642*, Hart Publishing, Oxford, 2015.....19

Edward J. Imwinkelreid, *Evidentiary Foundations* (LexisNexis, 6th ed., 2005) 206

Eoghan Casey, 'Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet' (Elsevier, 3rd ed, 2011) 92

Eoghan Casey, ed, *Handbook of Computer Crime Investgation: Forensic Tools and Technology* (Academic Press, United Kingdom, 2002).....148

Geoffrey Gilbert, *The Law of Evidence* (Catherine Lintot Publishing, United Kingdom, 1791) 27, 29, 34

George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008)11, 12, 226, 230, 238, 244

James B Thayer, *A Preliminary Treatise on Evidence at the Common Law* (Boston Little Brown, United States of America, 1898), 389.....21

Jeremy Bentham, A Treatise on Judicial Evidence Extracted from the Manuscripts of Jeremy Bentham, Esq (Baldwin, United Kingdom, 1st ed, 1825). 29

John Jay College of Criminal Justice, Towards Scalable E-discovery Using Content-based Hierarchical File Clustering (John Jay College of Criminal Justice, 2013) 158

John W Salmond, *Essays in Jurisprudence and Legal History* (Littleton Colorado F B Rothman, United States of America, 1987). 26

Julius Stone and William Wells, *Evidence Its History and Policies* (Butterworths, Australia: 1991) 16, 18, 19, 25, 33

Lee Andrew Bygrave, *The Meaning of 'Data' and Similar Concepts - An Issue of Growing Legal Importance*, In Cecilia Magnusson Sjöberg & Peter Wahlgren (ed.) Festskrift till Peter Seipel (Norstedts Juridik AB 2006) 117 – 126.....192

Michael T Clanchy, *From memory to written record: England, 1066-1307* (Cambridge Press, United Kingdom, 2nd ed, 1990).....17

Monica E. Seeley, Gerard N. Hargreaves, Managing in the Email Office (Routledge, United Kingdom, 2003) 85

Narasimha Karumanchi, Dr A. Damodaram and Dr M. Sreenivasa Rao, 'Elements of Computer Networking: An Integrated Approach', 2014 CareerMonk Publications.....72

Peter Singer & Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2009).....187

Stephen Mason (ed), *Electronic Evidence* (LexisNexis Butterworths, 3rd ed, 2012)38, 191, 192

Stephen Mason, *Electronic Signatures in* Law, 3rd ed, Cambridge, 2012 40

Stephen Odgers, *Uniform Evidence Law (*Thomson Reuters, Australia, 6th ed, 2004) .195, 198

Steve Wozniak with Gina Smith, 'iWoz: Computer Geek to Cult Icon: How I Invented the Personal Computer, Co-Founded Apple, and Had Fun Doing It', 2007 Steve Wozniak and Gina Smith 73

William Twining, Rethinking Evidence (North West University Press, Illinois, 2nd edition, 2006). 29

Articles

Aaron Upcroft, 'E-Commerce Global or Local? An Australian Case Study' (1999]) 10(1) *Journal of Law, Information and Science* 113.....50

Alberto Luis Zuppi, 'The Parol Evidence Rule: A Comparative Study of the Common Law, the Civil Law Tradition, and Lex Mercatoria' (2007) 35 *The Georgia Journal of International and Comparative Law* 233.....19, 21

Bernt Petter Jǿrgensen v DnB NOR Bank ASA by the Chairman of the Board (Trondheim District Court, 24 September 2004), 9 *Digital Evidence and Electronic Signature Law Review* (2012) 117-123 115

Bill Dawes, *Queensland MPs call for independent inquiry over Fitzgerald files shambles*, Image & Data Manager, March-April 2013 175

Bruce J Nikkel, 'Forensic acquisition and analysis of magnetic tapes' (2005) 2(1) *Digital Investigation* 8, 18.....76, 79

C Reed 'What is a Signature?' 2000(3) *Journal of Information, Law and Technology* located at <http://elj.warwick.ac.uk/jilt/00-3/reed.htm> at 11 September 2015 41

Cameron Spenceley, *Evidentiary Treatment of Computer-Produced Material: A Reliability Based Evaluation*, (PhD Thesis, University of Sydney, 2003) 9.....60, 61

Camille Cameron and Jonathan Liberman, 'Destruction of Documents Before Proceedings Commence: What is a Court to Do?', (2003) 27 *Melbourne University Law Review* 273 143

Christopher H. Boehning, and Daniel J. Toal., 'In Search of Better E-Discovery Methods' *New York Law Journal* (online) 23 April 2008.....157

David C. Blair., and M. E. Maron, 'An Evaluation of Retrieval Effectiveness for a Full-Text Document-Retrieval System' (1985) 28(3) *Communications of the ACM*, 289-299.....153

Edmund M. Morgan, 'The Jury and the Exclusionary Rules of Evidence' (1937) 4(2) *The University of Chicago Law Review* 247.....29, 34

Eilis S Magner 'The Best Evidence – Oral Testimony or Documentary Proof?' (1995) 18(1) *The University of New South Wales Law Journal* 67 29

Emmanuel Laryea, 'The Evidential Status of Electronic Data' (1999) 3 *National Law Review* 1.....38

Gordon V. Cormack and Maura R. Grossman, *Evaluation of Machine-Learning Protocols for Technology-Assisted Review in Electronic Discovery*, at: <http://www.wlrk.com/webdocs/wlrknew/AttorneyPubs/WLRK.23339.14.pdf> 11 September 2015 .....156, 163

Gordon V. Cormack and Maura R. Grossman, *Evaluation of Machine-Learning Protocols for Technology-Assisted Review in Electronic Discovery*, at: <http://www.wlrk.com/webdocs/wlrknew/AttorneyPubs/WLRK.23339.14.pdf> at 11 September 2015 234

Heather MacNeil, 'From the memory of the act itself. The evolution of written records as proof of jural acts in England, 11th to 17th century' (2006) 6 *Journal of Archival Science* 17, 18

Heather MacNeil, 'Providing Grounds for Trust: Developing Conceptual Requirements for the Long-term Preservation of Electronic Records,' (2000) 50 *Archivaria* 52–78 213

Heidi H. Harralson, 'Forensic document examination of electronically captured signatures', 9 *Digital Evidence and Electronic Signature Law Review* (2012) 67-73.....45

Hon. Andrew Peck, 'Search, Forward - Will manual document review and keyword searches be replaced by computer-assisted coding?' Law Technology News (online), 1 October 2011 http://www.lawtechnologynews.com/id=1202516530534/Search-Forward at 21 August 2015.....157

Ian Williams, "He Creditted More the Printed Booke – Common Lawyers Receptivity to Print 1550 to 1640" (2010) 28 *Law and History Review* 38.....19

James B Thayer, 'The Jury and its Development. II' (1892) 5 *Harvard Law Review* 29518, 21

Jason R Baron ed., 'The Sedona Conference Best Practices and Commentary on the Use of Search and Information Retrieval Methods in E-Discovery' (August 2007) 8 *The Sedona Conference Journal* 189.....153, 154, 156

Jason R. Baron, David D. Lewis & Douglas W. Oard, *TREC-2006 Legal Track Overview* (2006) Text REtrieval Conference < http://ece.umd.edu/~oard/pdf/trecov06.pdf> 154

Jason R. Baron, *Law in the Age of Exabytes: Some Further Thoughts on 'Information Inflation' and Current Issues in E-Discovery Search*, 17 Rich J.L & tech. 9 (2011).....5

John H Wigmore, 'A Brief History of the Parol Evidence Rule' (1904) 4 *Columbia Law Review* 17, 19, 21

John H Wigmore, 'The History of the Hearsay Rule' (1904) 7 *Harvard Law Review* 437 ...29, 30

John H. Langbein, 'Historical Foundations of the Law of Evidence: A View from the Ryder Sources' (1996) 96 *Columbia Law Review* 1168.....20

John W Salmond, 'The Superiority of Written Evidence' (1890) 6 Law Quarterly Review 75 .....26, 27

John W Strong and Edward W Cleary, 'The Best Evidence Rule: An Evaluation in Context' (1965) 51 *Iowa Law Review* 28

K.M Teeven, 'Seventeenth Century Evidentiary Concerns and the Statute of Frauds' (1983) 9 *Adelaide Law Review 252*.....24

Katherine Minotti, Comment, The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession, 60 S. C. L. Rev. 1057 (2009).....212

Ken Chasse, 'Electronic Records as Documentary Evidence' (2007) *Canadian Journal of Law and Technology*, 141.....117, 118, 238

Ken Chasse, *The Admissibility of Electronic Business Records*, (2011) 18:2 Canadian Journal of Law and Technology 105-191.....213

Lewis Evans, 'Economic Measurement and the Authorisation Process: The Expanding Place of Quantitative Analysis' (1999) 13 *Competition and Consumer Law Journal* 99 114

Luciana Duranti, Corinne Rogers and Anthony Sheppard, 'Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later' (2010) 70 *Archivaria* 95 .....213, 215

Maryke Silalahi Nuth, 'Unauthoized Use of Bank Cards With or Without the PIN: A Lost Case For The Customer?' 9 *Digital Evidence and Electronic Signature Law Review* (2012) 95-101 and Journal number 04-016794TVI-TRON.....115

Maura R. Grossman & Gordon V. Cormack, 'Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review' (2011) 17(3) *Richmond Journal of Law and Technology* 1 .....156, 161

Michael C. Weil, 'Dynamic Time & Date Stamp Analysis' (2002) 1(2) *International Journal of Digital Evidence* 150

New Zealand Law Society, '*Defining cloud computing*', <https://www.lawsociety.org.nz/lawtalk/lawtalk-archives/issue-845/defining-cloud-computing>, at 5 January 2016.....80

Nicolas Suzor., 'Privacy v Intellectual Property litigation: preliminary third party discovery on the Internet' (2004) 25 *Australian Bar Review* 254.....147

Olga I. Kudryavtseva, 'Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N KT-A 40/8531-03-IT', 5 *Digital Evidence and Electronic Signature Law Review* (2008) 149-151 47

Olga I. Kudryavtseva, 'The Use of Electronic Digital Signatures in Banking Relationships in the Russian Federation', 5 *Digital Evidence and Electronic Signature Law Review* (2008) 51-57 47

Paula Thomas and Alun Morris, 'An Investigation into the Development of an Anti-Forensic Tool to Obscure USB Flash Drive Device Information on a Windows XP Platform', (2008) *Third International Annual Workshop on Digital Forensics and Incident Analysis* 60-66.79

Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General.....84

Philip Turner, 'Digital provenance – interpretation, verification and corroboration' (2005) 2(1) *Digital Investigation: The International Journal of Digital Forensics & Incident Response* 45-49 211

Redgrave, J.M *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery*. (Ed), , 2nd ed, (2007) The Sedona Conference, Sedona.....155

Rodney McKemmish, 'IFIP International Federation for Information Processing' (2008) 285 *Advances in Digital Forensics IV* 3 124

Seth P. Berman, et al., Web 2.0: What's Evidence Between "Friends"?, Boston Bar J., Jan.–Feb. 2009.....212

Sharon Christensen, 'A National Law for Electronic Conveyancing - New Rules and Practices for Queensland' on *Thompson Reuters Online Insider* (24 May 2013) <http://blog.thomsonreuters.com.au/2013/05/a-national-law-for-electronic-conveyancing-new-rules-and-practices-for-queensland/> at 20 November 2014.....4, 54

Sharon Christensen, Bill Duncan & Rouhshi Low, 'Moving Queensland Property Transactions to the Digital Age: Can Writing and Signature Requirements be Fulfilled Electronically?' (2002) *Centre for Commercial and Property Law, Queensland University of Technology: Brisbane* 35 .....passim

Skogstad and Koppa, 'Admissibility of Business Entries' (1958) *Wisconsin Law Review* 2430

Stephen Mason and Nicholas Bohm, 'Commentary on Appeal Judgment'(2013) 10 *Digital Evidence and Electronic Signature Law Review* <http://journals.sas.ac.uk/deeslr/article/view/2041/1978> 43

Steven J. Murdoch, Saar Drimer, Ross Anderson and Mike Bond, 'Chip and PIN is Broken', 31st IEEE Symposium on Security and Privacy, IEEE Computer Society, 2010, pp 433-446; <http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf> as at 5 January 2016 43

The Hon. Justice Chesterman, *Managing Complex Litigation*, (Speech delivered at the Queensland Law Society's Continuing Legal Education Program, Brisbane, 22 October 2003); <http://www.sclqld.org.au/judicial-papers/judicial-profiles/profiles/rnchesterman/papers/1>, at 11 September 2015 181

The Hon. Marilyn Warren AC, The Litigation Contract: The Future Roles of Judges, Counsel and Lawyers in Litigation, Victorian Bar & Law Institute of Victoria Joint Conference High Stakes Law in Practice and the Courts, Friday 17 October 2014 182

Timothy S. Reiniger and Philip M. Marston, 'The Deed is Done: On-line Notarization Becomes a Reality', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 144-146.....54

Tony Cole 'The Parol Evidence Rule: A Comparative Analysis and Proposal' (2003) 26 *University of New South Wales* Law *Journal* 21

William M McGovern, 'Contract in Medieval England: The Necessity for Quid pro Quo and a Sum Certain' (1969) 13.3 *The American Journal of Legal History* 17

William M McGovern, 'Contract in Medieval England: Wager of Law and the Effect of Death' (1968) 54 *Iowa Law Review* 19 17

Yatan Dahiya and Sunita Sangwan, 'Developing and Enhancing the Security of Digital Evidence Bag' (2014) 1(2) *International Journal of Research Studies in Computer Science and Engineering (IJRSCSW)*.....11, 123

Commission Reports

Australian Law Reform Commission, *Evidence (Interim)*, Report No 26 (1985).....193, 202

Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Review of the Uniform Evidence Acts*, ALRC DP 69, VLRC DP (2005) 169

Australian Law Reform Commission, *Privilege in Perspective: Client Legal Privilege in Federal Investigations*, Report 107 (2007).....173, 174, 236

Australian Law Reform Commission, *Review of the Uniform Evidence Act*, DP 69 (July 2005) 2

Australian Law Reform Commission, *The Hearsay Rule in Civil Proceedings*, Report 216 (1993).....37, 66, 67, 68

Australian Law Reform Commission, *Uniform Evidence Law*, Report No 102 (2005)2, 36, 37, 38, 39, 40

English Law Commission, *Parol Evidence Rule*, Working Paper No. 154, (1986).....21

Queensland Law Reform Commission, *The Receipt of Evidence by Queensland Courts: Electronic Records*, Issues Paper WP No 52 (August 1998).....2

Queensland Law Reform Commission, *The Receipt of Evidence by Queensland Courts: Electronic Records*, QLRC WP 52, August 1998.....191

Court Rules & Practice Directions

Australia, Federal Court of Australia, *Federal Court Rules*.....98, 131

Australia, Supreme Court of New South Wales, *Practice Note SC Eq 11*, 22 March 2012.....9, 10, 127

Australia, Supreme Court of New South Wales, *Practice Note SC Eq 3*, 10 December 2008 .....133, 172

Australia, Supreme Court of New South Wales, SC Gen 7 *Supreme Court – Use of Technology*, 9 July 2008, commenced 1 August 2008 ..... 9, 130

Australia, Supreme Court of New South Wales, *Supreme Court Rules 1970* (NSW)..... 146

Australia, Supreme Court of Queensland, Practice Direction 2011/10 – Use of Technology for the Efficient Management of Documents in Litigation 130

Australia, Supreme Court of South Australia, *Supreme Court Civil Supplementary Rules 2014* (SA)..... 130, 134

Australia, Supreme Court of Tasmania, *Supreme Court Rules 2000* (Tas) 134

Australia, Supreme Court of the Northern Territory, Practice Direction No 2 of 2002, '*Guidelines for the Use of Information Technology in any Civil Matter*, 13 February 2002 130

Australia, Supreme Court of the Northern Territory, *Practice Direction No.2 of 2002 – Guidelines for the Use of Information Technology in Any Civil Matter*..... 135

Australia, Supreme Court of the Northern Territory, *Supreme Court Rules 2008* 135

Australia, Supreme Court of Victoria, Practice Note, No 1 of 2007 *Guidelines for the Use of Technology in any Civil Matter* 9, 130

Australia, Supreme Court of Victoria, *Supreme Court (General Civil Procedure) Rules 2005* (Vic) 133

Australia, Supreme Court of Western Australia *Technical Guide for Preparing and Submitting Documents for e-Trials* 134

Australia, Supreme Court of Western Australia, *Rules of the Supreme Court* 1971 (WA)... 134

Australia, Supreme Courts and District Courts of Western Australia *Technical Guide for Preparing and Submitting Documents for E-trials,* 24 September 2008..... 130

Australia, *Uniform Civil Procedure Rules 1999* (Qld) 133

Australia, *Uniform Civil Procedure Rules 2005* (NSW) 132

Canada, Courts of Alberta, *Alberta Rules of Court* 105

Supreme Court of Victoria *Practice Note No. 1 of 2007* 133

Standards

Australian Standard on records management, AS ISO 15489.1 - Part 1: General 13, 118

European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995. 84

NSW Registrar General, ARNECC Model Participation Rules, version 2, 18 March 2014 ..52, 53

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology & Department of Commerce United States of America, '*Secure Hash Standard*', Computer Security Resource Centre, March 2012 <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf> at 20 November 2014 ...65

The National Association of Testing Authorities, Australia, AS/NZS ISO/IEC 17799:2001 Information Technology – Code of practice for information security management.13, 118, 120

The National Association of Testing Authorities, Australia, HB171-2003 - Guidelines for the Management of IT Evidence.....13, 118

The Sedona Conference, *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery* (August 2007) <http://www.thesedonaconference.org>. 64, 65

The Sedona Conference, *Commentary on Inactive Information Sources*, (2009), <http://www.thesedonaconference.org> 69

The Sedona Conference, Electronic Document Retention and Production, Working Group 1 (2002). 61

Internet References

Andrew Combe, *Young Lawyers Seminar on Discovery*, Third Floor Wentworth Chambers <http://3wentworth.com.au/wp-content/uploads/2012/06/Young-Lawyers-Seminar-on-Discovery.pdf> at 11 September 2015 126

Australian Registrars' National Electronic Conveyancing Council (ARNECC) website: <http://www.arnecc.gov.au/> at 11 September 2015 51

Ben Grubb, 'George Brandis in "car crash" interview over controversial data retention regime', *The Sydney Morning Herald* (online) 7 August 2014 http://www.smh.com.au/digital-life/digital-life-news/george-brandis-in-car-crash-interview-over-controversial-data-retention-regime-20140806-101849.html at 11 September 2015.....62

Commonwealth Attorney-General's Department's website: <http://www.ag.gov.au/dataretention> at 11 September 2015 84

EDRM Website definition of email threading: http://www.edrm.net/resources/glossaries/grossman-cormack/email-threading at 12 January 2015.....159

EDRM Website definition of near duplicate detection: http://www.edrm.net/resources/glossaries/grossman-cormack/near-duplicate-detection at 12 January 2015 160

EDRM Website on Search Methodologies: <http://www.edrm.net/resources/guides/edrm-search-guide/search-methodologies> at 12 January 2015 159

Electronic Discovery Reference Model website: <http://www.edrm.net> at 11 September 2015 12

Ethan J, Wall, 'Social Networking Sites Look Like Plunder to Attorneys', *Daily Business Review* (online) February 20 2009 <http://www.dailybusinessreview.com/id=1202428417060/Social-Networking-Sites-Look-Like-Plunder-to-Attorneys?slreturn=20140928212644> 90

Facebook website: <http://www.facebook.com> at 11 September 2015 81

Federal Court website: <http://www.fedcourt.gov.au> at 11 September 2015 130

Flickr website: <http://www.flickr.com/> at 11 September 2015 89

Forensic Examination of Digital Evidence: A Guide for Law Enforcement (2004) <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf> at 11 September 2015 125

H. Marshall Jarrett and Michael W. Bailie, Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002) United States Department of Justice <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf > at 20 November 2014.....76

IETF Website: <http://www.ietf.org/> as at 11 September 2015.....65

Internet Engineering Task Force (IETF) website: <http://www.ietf.org> at 11 September 2015 151

LinkedIn website: <http://www.linkedin.com/> at 11 September 2015.....88

LIST website: <http://www.listgroup.org/the-rules/> at 21 September 2015 130

Max Duthie, 'The Subpoena and the Computer: A modern day tale of interrogation and oppression' (2005) *New South Wales Society for Computers and Law* < https://nswscl.org.au/index.php?option=com_content&view=article&id=120%3Athe-

subpoena-and-the-computer-a-modern-day-tale-of-interrogation-and-oppression&catid=27%3Amarch-2004-issue&Itemid=31> at 11 September 2015 147

Model Law on Electronic Commerce, (1996) UNCITRAL: 50

Myspace website: <http://www.myspace.com/> at 11 September 2015 88

National Archives of Australia, <http://www.naa.gov.au/Images/Check-up%202.0-All-Questions_tcm16-82787.pdf> at 11 September 2015.....81

National Institute of Standards and Technology website: <http://www.nist.gov/itl/cloud/index.cfm> at 25 July 2015.....80

Ontario Bar Association, Policy & Public Affairs, Ontario E-Discovery Implementation Committee, <http://www.oba.org/Advocacy/E-Discovery> 131

Pontello M., *TrIDEngine* (2012) Marco Pontello's Home Page <http://mark0.net/code-tridengine-e.html> at 11 September 2015.....128

Redit website: <http://www.reddit.com/> at 11 September 2015 88

Socha G. & Gelbman T., *EDRM Stages* (2014) The Electronic Discovery Reference Model <http://www.edrm.net/resources/edrm-stages-explained> at 11 September 2015 129

Supreme Court of New South Wales website: <http://www.lawlink.nsw.gov.au> at 11 September 2015 130

Supreme Court of Queensland website: <http://www.courts.qld.gov.au> at 11 September 2015 130

Supreme Court of South Australia website: <http://www.courts.sa.gov.au> at 11 September 2015.....130

Supreme Court of the Northern Territory website: <http://www.supremecourt.nt.gov.au> at 11 September 2015 130

Supreme Court of Victoria website: <http://www.supremecourt.vic.gov.au> at 11 September 2015.....130

Supreme Court of Western Australia website: <http://www.supremecourt.wa.gov.au> at 11 September 2015 130

Tash Shifrin, Is Web 2.0 a Security Risk? (2007) PC World <http://www.pcworld.com/article/130114/is_web_20_a_security_risk.html> 89

Teach-ICT.com: THE site for ICT education, <http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg10.htm> at 12 January 2015 79

Teach-ICT.com: THE site for ICT education, <http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg7.htm> at 12 January 2015.....78

Teach-ICT.com: THE site for ICT education, <http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg8.htm> at 12 January 2015.....78

Teach-ICT.com: THE site for ICT education, <http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg9.htm> at 12 January 2015.....78

Techopedia <https://www.techopedia.com/definition/25275/compactflash-cf> at 12 January 2015.....79

Techopedia: <https://www.techopedia.com/definition/24275/short-message-service--sms> at 12 January 2015 86

The Australian Government Gatekeeper PKI Framework, February 2009, <http://www.finance.gov.au/files/2012/04/Gatekeeper_PKI_Framework.pdf> at 11 September 2015 48

The Honourable J White, *Overview of the Evidence Act* (30 October 2010) Supreme Court of NSW <http://www.supremecourt.justice.nsw.gov.au/Documents/white301010.pdf> at 11 September 2015 56

The Sedona Conference website for a list of publications: <https://thesedonaconference.org/publications/> at 17 August 2015.....62

The Sedona Conference website: < http://thesedonaconference.org/> at 17 August 2015 ....61, 130

The Sedona Conference, '*Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*' (December 2013) <https://thesedonaconference.org/publications> at 17 August 2015.....64

The Sedona Conference, Commentary on ESI Evidence & Admissibility, March 2008, <http://www.thesedonaconference.org> 11 September 2015.....47

The Sedona Conference, *Commentary on Evidence & Admissibility*, (March 2008) <http://www.thesedonaconference.org> at 17 August 2015 127

The Sedona Principles Best Practices Recommendations and Principles Addressing Electronic Document Production (2nd ed: 2007), at <http://www.thesedonaconference.org> at 11 September 2015 .....62, 225

The Washington Post, 'U.S. battle over Microsoft e-mails could result in "global free-for-all"', <https://www.washingtonpost.com/world/national-security/us-battle-over-microsoft-e-mails-could-result-in-global-free-for-all/2015/09/09/f8dcbf1e-5722-11e5-abe9-27d53f250b11_story.html>; as at 5 January 2016 82

Twitter voted top English word', *The Telegraph* (online), 30 November 2009 <http://www.telegraph.co.uk/technology/twitter/6685906/Twitter-voted-top-English-word.html> at 11 September 2015 89

Twitter website: <http://www.twitter.com/> at 11 September 2015 88

Wikipedia website: <http://www.wikipedia.org/> at 11 September 2015 89

WiseGEEK: <http://www.wisegeek.com/what-is-a-sim-card.htm> at 12 January 2015 80

Youtube website: <http://www.youtube.com/> at 11 September 2015 89

Other Authorities

Australian Privacy Principles; extracted from Privacy Act 1988 (Cth) 90

Judge David Harvey, *Collisions in the Digital Paradigm: Legal Rules and New Technologies*, 3rd Annual New Zealand Law & Technology Conference, 18 March 2015 ..... 60, 238

Law Society of England & Wales, '*Cloud Computing*' Practice note, 7 April 2014, http://www.lawsociety.org.uk/support-services/advice/practice-notes/cloud-computing/, at 5 January 2016 80

Law Society of England & Wales, 'Social Media' Practice Note, 18 June 2015, <http://www.lawsociety.org.uk/support-services/advice/practice-notes/social-media/> at 5 January 2016 88

Litigation Law and Practice Committee of the Law Society of New South Wales, Submission E 103, 22 39

Lord Justice Jackson, Review of Civil Litigation Costs: Final Report, 21st December 2009 127

Office of the Victorian Privacy Commissioner, Submission E 115, 30 September 2005 39

Pan Macmillan Australia, The Macquarie Dictionary 2013, 6th edn (1 September 2013), Australia's National Dictionary 136

Queensland Parliamentary Crime and Corruption Committee, Inquiry into the CMC's release and destruction of Fitzgerald inquiry documents, hearings conducted on Wednesday 13 March to Friday 22 March, and on Thursday 28 March 2013, <https://www.parliament.qld.gov.au/work-of-